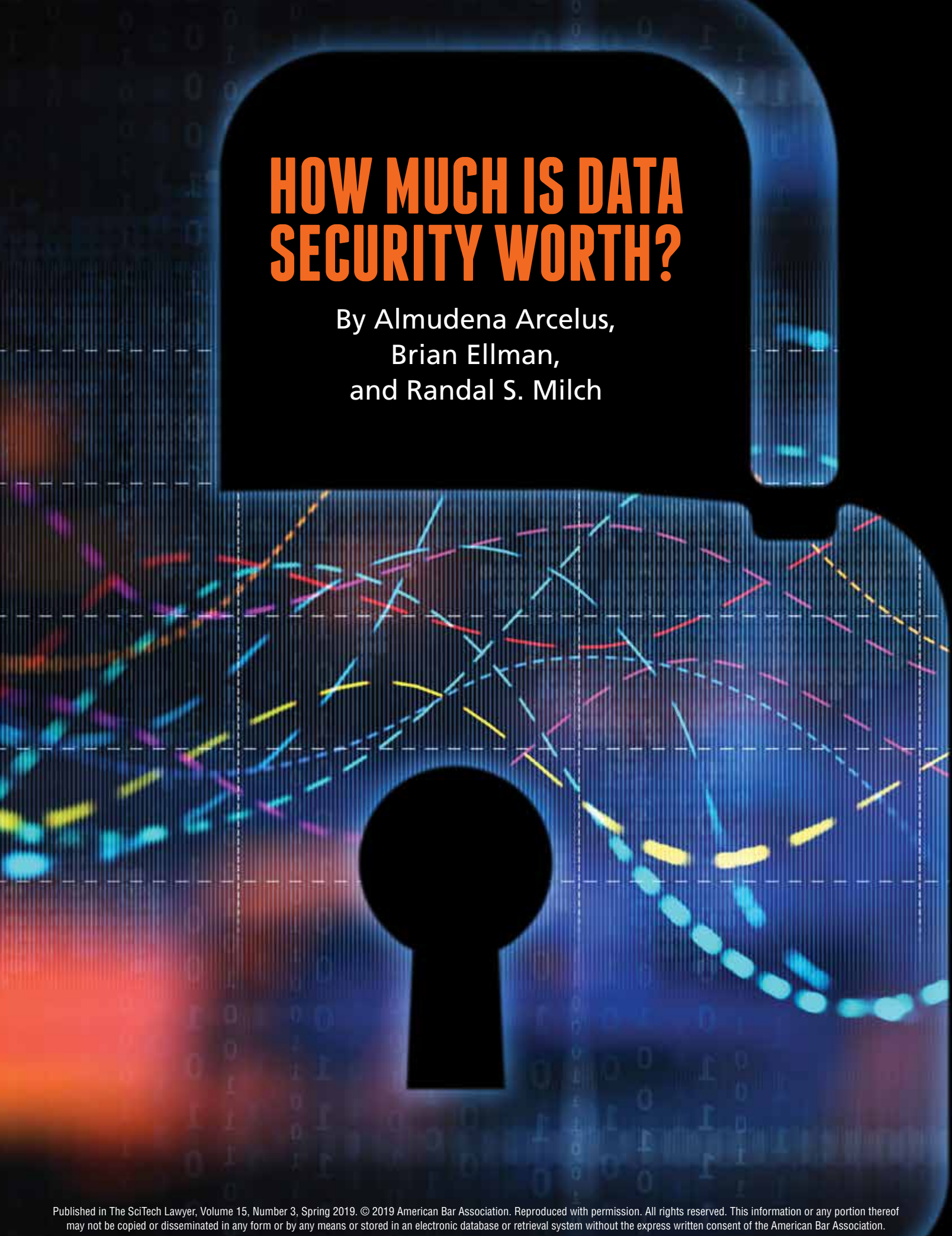


HOW MUCH IS DATA SECURITY WORTH?

By Almudena Arcelus,
Brian Ellman,
and Randal S. Milch

Data—an entity's information assets—are earning a reputation as the new strategic currency for many organizations. In this era of big data and interconnectivity, critical information assets often are at the core of evolving business models, and the value of data is increasing daily.

By the same token, data are making organizations more vulnerable. Those information assets, especially personal and financial customer data, expose their stewards to greater risk, leaving them vulnerable to increasingly sophisticated cyberattacks or larger, more harmful lapses in security.

This article focuses on one method for assessing the value of investing in cybersecurity measures to protect these data against attacks and exploits aimed at critical information assets. While it is written from the perspective of commercial business organizations, the approach should find applicability across the entirety of the "information ecosystem."

The old rules for balancing risk and reward must adapt to the realities, and the systemic threats, of a data-centric cyber-world. Corporate and financial decision makers recognize the importance of investing in products and strategies for preventing and mitigating cyber-risks. However, determining the right level of investment can be challenging, and the consequences of getting it wrong can be severe. The probability of a company suffering a breach is rising swiftly, and the costs of a breach are skyrocketing. Each company must assess its own level of risk: How likely is a breach to occur, and what would be the consequences? Each company must also constantly evaluate the security measures it has in place and determine whether the cost of improvement outweighs the risk of a breach.

In a world in which the methods used by data thieves are evolving faster than corporate defenses, how can a rational, profit-maximizing firm stay ahead without incurring endless costs? One answer may lie in borrowing an approach from the antitrust courtroom—applying a "rule of reason" to weigh the costs of increased security against the economic benefits of reducing the risk and consequences of a breach.

Corporate Information Assets Are Threatened

The topic of data security remains firmly in the news, with reports of new data breaches appearing regularly.[1] Although the impacts of such high-profile incidents as the Equifax or, more recently, the Marriott breaches remain to be sorted out, the consequences of other breaches can provide examples that highlight the importance of taking a detailed look at a business's data security practices and investments.

For instance, in May of 2017, the retailer Target agreed to pay $18.5 million in a consumer data breach settlement with 47 states.[2] Four years earlier, cyber attackers used stolen credentials and malware to access Target's customer service database. Before they were detected, the attackers mined credit card information on over 40 million customer accounts and contact information for more than 60 million customers.

The May 2017 settlement was only one of the costs incurred by Target in the aftermath of the cyberattack. In all, Target estimated that the breach cost the company more than $200 million,[3] including a separate multimillion-dollar settlement in a class action brought by the merchant banks covering the alleged fraudulent activity on the credit card accounts; notification and credit monitoring costs; and the implementation of a comprehensive information security program.

Target is far from the only company to make headlines because of data security. During the past few years, the public has been made aware of massive data breaches at Home Depot, Marriott, and Yahoo!, among many others. In one high-profile case, Equifax's revelation that it had suffered a massive data breach of credit information led to widespread examination both of its response and its management. Within three weeks of the breach announcement, Equifax's CEO, chief information officer, and chief security officer resigned.[4]

A data breach doesn't have to be on the scale of an Equifax or a Target to be troublesome and costly to the company, however. According to one study of data security costs, in 2016 U.S. companies that had fewer than 100,000 records affected by a data breach estimated breach-related costs to be more than $7 million, on average.[5]

How Much Is Enough? Applying the "Rule of Reason" to Data Security

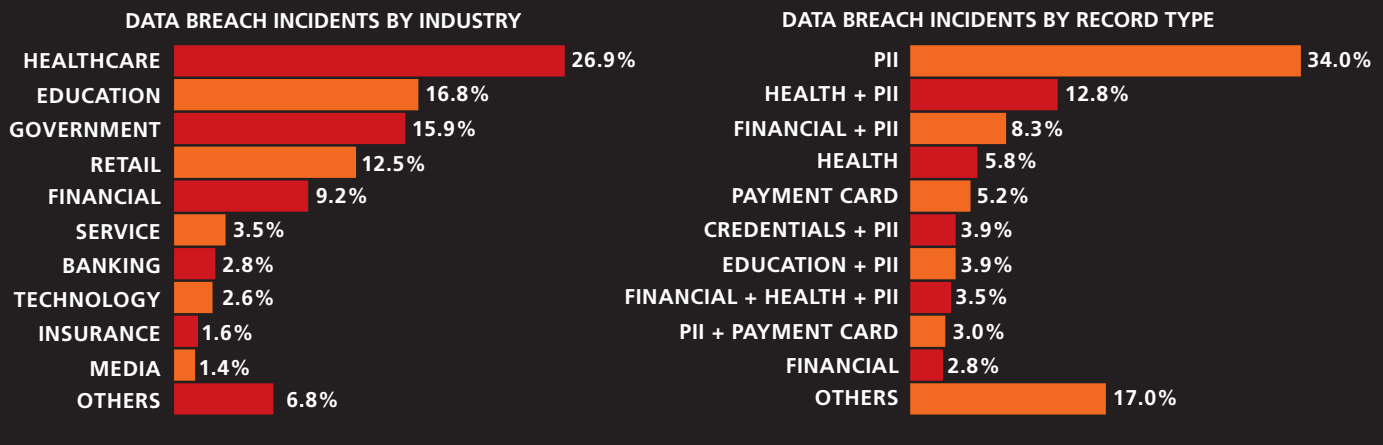
Economic theory suggests that a "rational" firm will enhance data security only up to the point where the cost of the additional security remains less than the probabilistic cost of a breach. In finding that tipping point, corporate decision makers may find it helpful to take guidance from competition regulation and apply a fact-based "rule of reason" approach.

In antitrust litigation, an action that is not illegal *per se* is deemed anticompetitive only if the economic consequences of the action result in "unreasonable" restraints of trade. The "rule of reason" approach acknowledges that, even if anticompetitive actions can be proven, they may be at least partially offset by procompetitive effects. Of course, the key debate in any such case is what counts towards determining the reasonableness of the action at issue.

"Reasonableness" is also a touchstone for the regulatory and litigation aftermaths of a data breach. For example, the Federal Trade Commission (FTC) took action against the hotel chain Wyndham when the information systems of Wyndham hotels were hacked on three separate occasions,

Almudena Arcelus *(almudena.arcelus@analysisgroup.com) is a Principal and* ***Brian Ellman*** *(brian.ellman@analysisgroup.com) is a Vice President with Analysis Group, Inc.* ***Randal S. Milch*** *is an Analysis Group Affiliate and Co-Chair at the NYU Center for Cybersecurity.*

FIGURE 1. DATA BREACH INCIDENTS 2005-2015



PII = Personally Identifiable Information (e.g., names, addresses, Social Security numbers)
Source: Follow the Data: Analyzing Breaches by Industry,
Trend Micro Analysis of Privacy Rights Clearinghouse, 2005-2015 Data Breach Records

resulting in the theft of over half a million customers' personal information. The FTC alleged that Wyndham failed to provide "reasonable and appropriate security" measures,[6] even though Wyndham claimed it had followed "industry standard practices,"[7] and that Wyndham's failure to provide "reasonable" information security violated the Federal Trade Commission Act, prohibiting unfair or deceptive acts affecting commerce.

A key element in the decision against Wyndham was the history of rulings that substantial harm to consumers could serve as the basis for a determination of an unfair practice. But case law also requires that the consequences of an action "must not be outweighed by any countervailing benefits to consumers or competition that the practice produces"—echoing the FTC's statutory standard with respect to an unfair practice.[8] Hence, the decision in the Wyndham case states that "the relevant inquiry here is a cost-benefit analysis. . ." that considers factors, including "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[9]

Using the "rule of reason" approach, companies will need to determine the point at which the incremental benefits from additional cybersecurity outweigh the cost required to obtain those benefits. To make "rational" business decisions, companies need a *risk-adjusted* measure that helps them understand their risk exposure. In other words, decision makers need to ask: Do our current investments adequately address the risk to our business of incurring costs associated with a breach of our data assets?

Solving the Data Security Equation

In considering whether to beef up investment in data security, firms may find it helpful to solve for an equation that reflects the amount up to which an economically rational firm would be willing to spend in incremental security based on the probabilistic cost of a breach:

Cost of incremental security ≤ *probability of breach* × *cost of breach*

When applying this equation, companies should consider all three of its components:

1. Probability of a breach, answering the question, "How likely are we to suffer a breach?"
2. Cost of a breach, answering the question, "What would the economic impact be on our company if we did suffer a breach?"
3. Cost of incremental security, answering the question, "What additional measures could we take to guard against a breach or reduce its impact to our business, and at what cost?"

We will examine each of these components in the following sections.

1. Determining the Probability of a Data Breach

Cost of incremental security ≤ ***probability of breach*** × *cost of breach*

A business's risk exposure starts with an assessment of the probability that the company will experience a data breach. The probability of a breach is based on a number of factors, including the type of data a company stores; the assets (e.g., computers, personal devices, phone systems, cloud services) a company uses to store and access data; the company's industry; and the preventive measures already taken. Each company should also consider potential vulnerabilities related to its broader ecosystem, such as the security risks presented by vendors or partners that may have access to its data.

Research suggests that a number of factors are correlated with an increased probability that a business will suffer a data breach. For example, as shown in Figure 1, companies in certain industries and holding or providing access to certain types of data have proven more vulnerable than others. Unsurprisingly, companies holding or with access to personally identifiable information, health, financial, and/or payment card information are prime breach targets.[10] This suggests that, in solving the data security equation, companies must first perform a comprehensive audit of the types of information they hold or may have access to, and then assign different weights to these different types of data, reflecting the relative risk.[11]

However, factors other than a company's industry, such as firm size or function, may affect the probability that it will be targeted.[12] Even among companies in the same industry that collect and maintain similar types of data, the risk of a data breach can vary based on company-specific characteristics. A holistic assessment of the company's breach probability must also consider how susceptible the company is to an attempt to breach its data infrastructure, such as corporate espionage, political "hacktivism", or a personal vendetta.

Finally, the technology a company employs and its security practices can either increase or decrease the probability of a breach. The type and number of assets that can be the source of a breach—such as databases, servers, laptops, and transaction systems—as well as the presence or absence of formal security procedures, can all affect a company's vulnerability, as can the security risks presented by the broader data ecosystem through which other partners can access customer data.

In general, a company's risk may increase depending on how many records or accounts it maintains or to which it has access, how sensitive its data are, and how well it protects its points of vulnerability.

2. Estimating the Cost of a Data Breach

Cost of incremental security ≤ *probability of breach* × ***cost of breach***

The type and amount of data that may be exposed in a breach will strongly influence related costs, and companies may need to prepare estimates or develop worst-case scenarios when modeling them. To develop a risk-adjusted measure, the probability of a breach can be multiplied by the estimated cost of a discrete incident. A company will need to determine what economic harm is likely to be caused by a data breach.

The cost of a breach encompasses all direct and indirect costs that a company incurs to respond to and recover from a data breach after it occurs. This comes in two primary forms: lost business and the costs associated with responding to the breach. The latter category of costs includes ex-post costs; detection and escalation costs involved with managing the company's response; and activities related to notifying potentially affected customers and responding to regulatory requirements. (See Figure 2 on p. 14.)

Lost business can represent one of the more serious risks to financial performance. A tarnished reputation can lead to higher customer turnover, difficulty and increased costs associated with acquiring new customers, and diminished goodwill. However, these effects also are likely to fade over time; how quickly they diminish depends in part on the speed, effectiveness, and transparency of the company's response. Estimating the impact on financial performance over time requires a sophisticated understanding of revenue drivers, market position, brand strength, competitive effects, and many other factors.

Breach-specific costs can be in the form of ex-post costs, detection and escalation costs, and notification-related activities. Ex-post costs are those incurred by actions taken in response to the event itself, such as ramping up customer service and other internal resources to mitigate the damage and retaining identity protection services.

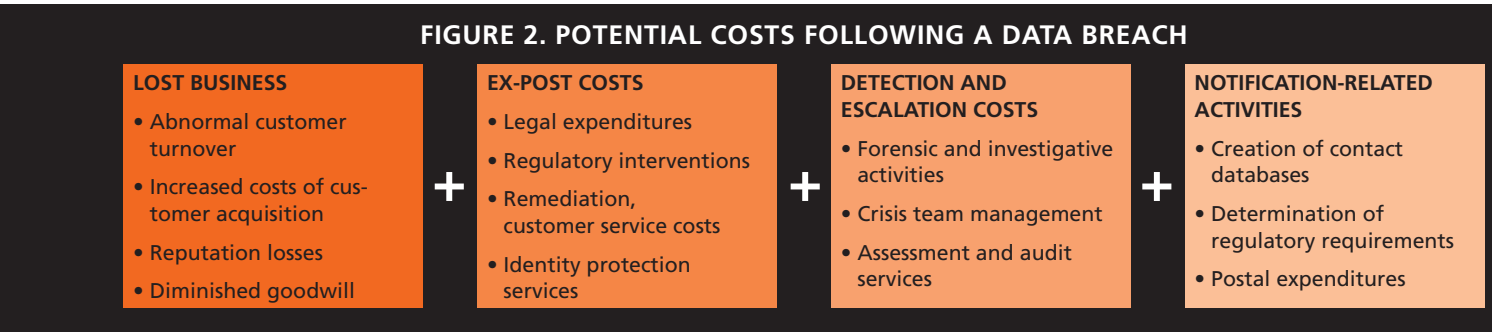
Ex-post cost estimates should also consider potential legal fees for defending the company against civil actions and regulatory investigations, as well as any penalties, damages, or settlement costs. For many years, a requirement to show actual injury arising from a breach kept numerous consumer plaintiffs out of court. However, after the Supreme Court's ruling in *Spokeo, Inc. v. Robins*,[13] while a data privacy claim must describe a "concrete" injury, those injuries can be intangible or contain allegations showing a future "material risk of harm."[14] While companies will still win occasional standing victories,[15] it is likely that future breach litigation will reach the merits and center more on the reasonableness of a breached company's cybersecurity measures.

In terms of detection and escalation costs, the company will likely need to hire outside experts to identify the source of the breach and recommend measures to contain and repair it, and develop appropriate responses. For example, in the immediate aftermath of the breach announcement, Equifax created a website for consumers to determine whether they were impacted and learn how to protect themselves; offered a free credit file monitoring and identity theft protection program to all U.S. consumers for one year; and set up a call center to assist consumers. According to one estimate, Equifax's "Premier" credit monitoring and identity-protection offer for 250 million U.S. residents over the age of 18 potentially represented nearly $60 billion worth of services.[16]

Finally, a company will need to develop and implement a plan for notifying affected parties of the breach and continuously communicating its response. The 50 states, Washington D.C., Puerto Rico, Guam, and the Virgin Islands impose differing legal requirements for post-breach notification. A company will incur costs as part of its effort to ensure compliance with all relevant jurisdictions' notification requirements; failure to comply in the event of a breach will result in substantial additional costs.

As a result, any assessment of likely and potential costs associated with responding to a breach will necessarily vary depending on the type of business and the nature of the breach.

FIGURE 2. POTENTIAL COSTS FOLLOWING A DATA BREACH



3. Estimating the Costs of Increased Security

Cost of incremental security ≤ *probability (breach)* × *cost of breach*

The ultimate cost of incremental security is based on the actions a company may take to protect itself against and ameliorate the effects of a future breach. In determining a risk-adjusted cost of a data breach, a company will need to evaluate the security measures it already has in place. After assessing the effectiveness of its data security measures relative to the risks it faces, a business can then identify and evaluate its options for addressing existing or potential weaknesses. Finally, it can estimate the cost of making those improvements, and compare those costs to the reduced level of risk resulting from improvements in data security. Here again, a company must be able to gauge whether action is justified from a business perspective, while taking into account a shifting landscape in terms of potential threats and available remedies.

As more instances of data breaches appear in headlines and reach the courts, the demand for cybersecurity products and services will continue to increase. According to one estimate, the global cybersecurity market is expected grow from about $138 billion in 2017 to nearly $232 billion by 2022.[17]

Accordingly, supply of cybersecurity products will likely rise to meet the increasing demand. New companies will enter the marketplace, and established companies will expand product lines and offer enhanced capabilities. In addition, new products are being developed that build on advanced data technologies, such as big data analytics to monitor and manage identity and access patterns, and cloud computing to allow better linkages among existing and emerging tools. Even though many of these products will fail, one result of this proliferation may be that unit costs for incremental investment in firm-level cybersecurity will start to decline, as supply-side reaction by businesses offering data privacy solutions makes cybersecurity more cost-effective.

Conclusion: Striking the Balance

When it comes to solving the data security equation, businesses will need to continuously reevaluate trade-offs between the level of risk they face and the costs of mitigating those risks. More and more, competition is being defined in terms of the ability to leverage larger volumes of increasingly detailed customer data in order to translate highly individualized data into new products or effective targeted marketing. The more information a business has, however, the more it is at risk to those who seek to exploit the data illegitimately.

Solving the cybersecurity equation involves determining the level at which the marginal benefits of providing incremental security equal or exceed the cost of providing it. To keep on top of the challenge, a company should start by asking itself a few key questions:

- What data do we currently collect and maintain, and how are the data stored and accessed? Which technology assets are most vulnerable?
- How necessary are the data for our business and for creating new sources of value for our customers? Can our exposure be reduced if we are more selective about the data we keep?
- Does our industry, firm size, and business model leave us any more or less vulnerable to a breach and/or associated costs?
- Do our data practices make us a more or less attractive target for illegal activity?
- Which measures should be implemented to lower the probability of a high-cost breach and to reduce the effects of a breach on our business and customers?

Making these types of assessments provides the starting point for employing a "rule of reason" approach to determine whether the potential costs of a breach justify additional investment in security and prevention.◆

Endnotes

1. A "breach" is a cybersecurity incident in which one or more information security vulnerabilities are exploited with the result that the confidentiality, integrity, or accessibility of an information system, or the information on that system, is compromised. Most frequently, a breach involves the exfiltration of information from a system, but it could also involve taking down a system or manipulating data on a system.

2. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

3. https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting.

4. https://www.bloomberg.com/news/articles/2017-09-26/equifax-ceo-smith-resigns-barros-named-interim-chief-after-hack.

5. Ponemon Institute, 2017 Cost of Data Breach Study: United States, June 2017.

6. *Fed. Trade Comm. v. Wyndham Worldwide Corp.* (FAC ¶ 24).

7. *Id.* ¶ 21.

8. 15 U.S.C. §45(n) states that "The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *See* https://www.law.cornell.edu/uscode/text/15/45.

9. *Fed. Trade Comm. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 259 (3d Cir. 2015). Although the Eleventh Circuit has called into question the enforceability of the FTC's reasonableness approach (*see* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018)), reasonableness remains the statutory standard in the financial industry as part of the Gramm-Leach-Bliley Safeguards Rule, as well as the common law standard for negligence in breach litigation.

10. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf.

11. The study also found that health care companies were the most likely to have suffered a data breach over a 10-year period, accounting for slightly more than a quarter of all incidents. Education and government were approximately equally likely to have incidents, followed by the retail and financial sectors. Given the breadth of personal data collected and maintained by such institutions, it is not surprising that they would be a primary target for hackers.

12. https://hub.jhu.edu/2017/04/05/hospitals-at-risk-of-data-breach-patient-records.

13. 138 S. Ct. 931 (2018), http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins.

14. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); *In re* Horizon Healthcare Serv. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).

15. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 273–76 (4th Cir. 2017) (increased risk of future identity theft alone insufficient to establish injury-in-fact).

16. https://iapp.org/news/a/equifax-data-breach-affects-143-million-consumers

17. http://www.marketsandmarkets.com/PressReleases/cyber-security.asp.