Harvard Business Review

SECURITY & PRIVACY

Research: A Strong Privacy Policy Can Save Your Company Millions

by Kelly D. Martin, Abhishek Borah, and Robert W. Palmatier

FEBRUARY 15, 2018

OSMAN RANA/HAYON THAPALIYA/UNSPLASH

Cyberattacks are on the rise, with over 1,000 data breaches occurring at U.S. organizations in 2016 alone, most often through hacking or external theft. And it isn't only violated firms that are hurt by these incidents. Studying hundreds of data breaches, our research has found that they create significant ripples that affect other companies in the industry.

Our research shows that data breaches sometimes harm a firm's close rivals (due to spillover effects), but sometimes help them (due to competitive effects). What is more, we found that a good corporate privacy policy can shield firms from the financial harm posed by a data breach — by offering customers transparency and control over their personal information — while a flawed policy can exacerbate the problems caused by a breach. Together, this evidence is the first to show that a firm's close rivals are directly, financially affected by its data breach and also to offer actionable solutions that could save some companies hundreds of millions of dollars.

Our research shows that sometimes a breach creates spillover, where investors perceive a guilt-by-association effect that harms the breached firm's close rivals. For an example of competitor harm due to these spillover effects, consider the July 2012 Nvidia data breach, which affected 400,000 user accounts. Its rival Advanced Micro Devices (AMD) lost about $48 million on the event day (-1.4% drop in stock price) from the spillover effects of Nvidia's breach, controlling for overall market effects. That is, when removing from our analyses all other events that could have influenced AMD's stock drop, such as dividend declarations, contract signings, earnings information, or mergers and acquisitions, we find that clear and significant harm occurred from Nvidia's data breach.

In fact, the spillover effects across our sample evidenced a drop in stock price that averaged more than $8 million in losses for rival firms where no such data breach occurred. Our results show the financial hit to these rivals' stock prices can be detected for several days

after the data breach before eventually stabilizing.

Yet a breach can sometimes help a close rival, creating beneficial competitive effects. Consider the massive Anthem data breach in February 2015, which affected as many as 80 million customers. The high severity of this breach led rival Aetna to gain about $745 million (2.2% increase in stock prices) on the event day due to competitive effects, again controlling for overall market effects. In this situation, a data breach of this scale makes investors worry about customers mass defecting to competitors, thus providing a positive boost to a close competitor's stock price.

Our research shows that the severity of, or number of customers affected by, a breach is a key to understanding whether close rivals will be harmed or helped by their competitor's bad fortune. As the number of customers harmed by the breach increases, stock market effects for the firm's rivals go from negative to positive, as competitive effects become more dominant. This suggests that smaller breaches signal that others in the industry may also be vulnerable to hacking. However, large data breaches create the impression that the breached firm is in a unique amount of trouble. Our research shows that in large data breaches, customers increasingly desire to leave the breached firm. Expected switching behavior ultimately benefits the breached firm's competitors, as captured in their stock returns.

The good news is that firms are not powerless against these data breach effects. There are actionable strategies they can use to protect or inoculate themselves from their own or a rival's breach. Using studies querying hundreds of customers that we recruited on Amazon Mechanical Turk, coupled with stock data analysis of hundreds of companies over the past decade, our research finds that firms can protect themselves from data breach harm by implementing two important privacy-focused practices that benefit customers.

First, they can clearly explain to customers how they are using and sharing their data. Transparent privacy practices tell customers what specific information companies capture and how they use it (for example, IP address, search history, promotions, information being sold to third parties). Second, firms can give customers ample control over the use and sharing of their data. Control is endowed through giving customer opportunities to opt out of the firm's data practices (promotions, sharing with partners, selling). Together, these measures were perceived to effectively empower customers, giving them greater knowledge and the ability to have a say in business practices.

Why Study Privacy Policies?

Although companies can provide transparency and control through various customer communications, the formalized and codified ways they do this is their privacy policies. These policies are important customer communication tools because the firm has legally agreed to abide by them. Regardless of what a company might message about data privacy in other ways, what must be put into practice is formally documented in the privacy policy. When customers are in doubt about their personal information, company messaging commonly refers them back to the privacy policy. Finally, a recent review of data privacy research in marketing found that customers do, in fact, have a good idea of a firm's data practices as captured in a firm's privacy policy — even if they do not read the privacy

When a firm had transparent privacy practices, customers in our studies felt they had the knowledge to make an informed decision about sharing their personal data. When a firm's privacy practices offered control, customers knew they had the ability to change their preferences about what and how they share their information. In our studies, customers did not punish breached firms that provided both transparency and control. Empowered customers are more willing to share information and are more forgiving of data privacy breaches, remaining loyal after the fact, as we learned. Customers of firms that offer high transparency and control reported feeling less violated from big data practices, attested to being more

policy. Because privacy policies are simply a documentation of all company privacy practices, customers that are familiar with a given company and its approach to privacy have a highly accurate sense of what is in the policy. Again, our research with hundreds of customers confirmed this knowledge.

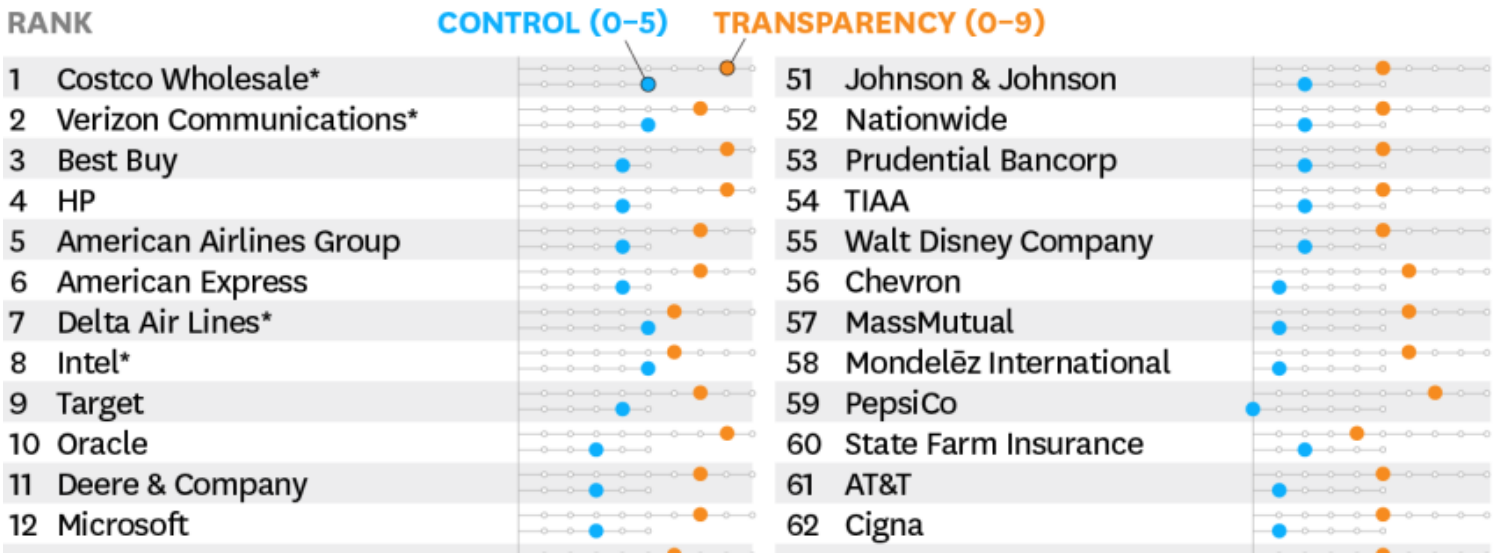
trusting, provided more-accurate data to the firm, and were more likely to generate positive word of mouth.

Firms high on these two dimensions also were buffered from stock price damage during data breaches, either their own or rivals'. Yet only about 10% of Fortune 500 firms fit this profile.

To study how a firm implements practices that provide transparency and control, we needed to look at the documented ways in which companies explain their approach to customer data privacy. By studying their use of transparency and control in their privacy policies, we wanted to understand how protected Fortune 100 firms were from the negative effects of data breaches. Our research team combed the privacy policies of all Fortune 100 firms to gain insights.

How Good Are the Fortune 100's Privacy Policies?

A ranking of how transparent each company's policy is, and how much control it gives customers.



*THE PRIVACY POLICIES OF THESE COMPANIES OFFER ADDITIONAL OPT-OUTS THAT DID NOT FACTOR INTO OUR RANKING.
SOURCE KELLY D. MARTIN, ROBERT W. PALMATIER, AND ABHISHEK BORAH

Our findings show that some firms provide high levels of data transparency and control, and would be protected from data breaches. (See our ranking in the exhibit "How Good Are the Fortune 100's Privacy Policies?") Top-ranked firms such as Costco, Verizon, and HP would be shielded from spillover effects were a close competitor to experience a data breach. These firms clearly convey what information they capture and how they capture it, while offering their customers substantial control or say in that information's sharing and use.

On the other end of the ranking are firms such as Citigroup, Morgan Stanley, and HCA. In 2011 Citigroup experienced a data breach of 146,000 customer records and suffered a $1.3 billion stock value loss. According to our analysis, if Citigroup had embraced practices of high transparency and high control, it would have suffered a loss of only about $16 million in stock value. That is, Citigroup might have saved about $820 million had it simply offered its customers high transparency and control. In response to this breach, Citigroup spent $250 million on cybersecurity systems and hired an additional 1,000 IT professionals. Yet our coding of its practices reveals that, as recently as 2016, Citi still was not providing high levels of transparency and control. Thus, while its enhanced IT safeguards may be sound, our research shows the company remains at risk should a competitor suffer a breach.

Company Ranking Methodology

We created *transparency* and *control* variables with procedures that employed a mix of automation and manual coding of companies' actual privacy policies.

First, we captured all the relevant URLs pertaining to firms' privacy policies that were in effect on January 1, 2016. We developed a Python code

Looking across the rankings, other firms appear to offer one of these aspects to customers. For example, some firms provide transparency, but fail to give customers the ability to act on this information (low control). In our research, this approach was poorly received by customers.

that visited all valid snapshots of each Fortune 500 firm's privacy policy to extract that closest to our date of interest. In order to ensure the correct URLs were downloaded and parsed, a manual layer of quality check was performed. Specifically, a random 5% of the URLs were checked to find if there were any errors in the code, and the errors were corrected. We then resampled the URLs and found no errors. This process ensured that we correctly retrieved the privacy policy. Third, after obtaining the relevant privacy policy, we employed manual coding to construct the transparency and control variables, which consisted of carefully reading each privacy policy and using a coding schema to create count scores for transparency and control. For the variables that required coding of events, we followed standard procedures for textual coding.

Specifically, for the textual coding procedure, we employed two research assistants who were blind to the study hypothesis. Prior to coding the privacy policies, the two research assistants were independently trained on a sample of privacy policies (that were not part of the final sample) to use the coding scheme. One of the authors checked to ensure the research assistants understood the coding scheme. After obtaining all the privacy

Finally, firms that neither tell customers how they use their data nor offer any control are at the greatest risk of financial harm. Our privacy analysis showed that an overwhelming 80% of Fortune 500 firms fall into this category. In our study, firms that failed to explain their data privacy practices had a 1.5 times larger drop in stock price than firms with high transparency, while firms that provided customers high control had no significant change in their stock price after a data breach.

Ultimately, firms can use data privacy practices to protect themselves from the spillover effects of competitors' privacy failures, but their efforts to do so need to be meaningful. They must clearly explain to customers the ways in which they will access, use, share, and protect customer information, and it must go hand in hand with giving customers control over these data uses. Failure to do so leaves a firm susceptible to risk from multiple harms.

Editor's note: Every ranking or index is just one way to analyze and compare companies or places, based on a specific methodology and

policies, each research assistant independently coded them. Finally, after all the privacy policies were coded, the interrater agreement between the two research assistants was greater than 85%, and all disagreements were resolved through discussion with the first author.

For the transparency variable, we used a count of the dummy variables across multiple elements of the privacy policy that signal openness and willingness to provide information to customers. Specifically, we coded whether the firm (1) explains its opt-out policy, (2) explains how it captures data, (3) explains how it uses data, (4) explains its use of tracking tools, (5) explains the value customers receive from providing their information, (6) explains its data sharing with third parties, (7) explains its data encryption practices, (8) provides contact information for privacy requests, and (9) discusses protections if data is compromised. If a firm's privacy policy had all nine characteristics, the policy earned a transparency score of nine.

To create the control variable, we counted the number of opt-out choices in the firm's privacy policy. Specifically, we coded whether the customer can opt out of (1) marketing communications, (2) saving data usage (for example, search history), (3)

data set. At HBR, we believe that a well-designed index can provide useful insights, even though by definition it is a snapshot of a bigger picture. We always urge you to read the methodology carefully.

storing personal information (for example, credit card number), (4) sharing data with third parties, and (5) tracking. If a firm's privacy policy had all five characteristics, the policy earned a control score of five. Note that we also counted opt-outs that were not on this list, but that were featured as part of the firm's privacy policy. Four firms included additional data collection or data-use opt-outs beyond our five characteristics. These were firm-specific opt-outs that enabled greater customer control, but did not warrant separate opt-out categories for the entire sample of firms.

To create our rankings, we compiled the summed scores of transparency and control for all firms. Rankings were achieved by summing the combined transparency and control scores. It follows that some firms had identical scores on both dimensions, and in such cases they appear according to alphabetical order in the ranking.

Kelly D. Martin is an associate professor of marketing and Dean's Distinguished Research Fellow at Colorado State University.

Abhishek Borah is an assistant professor of marketing at the University of Washington's Michael G. Foster School of Business.

Robert W. Palmatier is a professor of marketing and the John C. Narver Chair in Business Administration at the University of Washington's Michael G. Foster School of Business.

This article is about SECURITY & PRIVACY

⊕ **FOLLOW** THIS TOPIC

Related Topics: RISK MANAGEMENT | CUSTOMERS

Comments

Leave a Comment

POST

0 COMMENTS

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must