Building consumer trust

Protecting personal data in the consumer product industry

Deloitte University Press

About the authors

Pat Conroy

As the national leader of one of the industry practices at Deloitte, which employs more than 2,400 professionals, Pat Conroy (Deloitte LLP) is responsible for building eminence for the consumer products industry practice and leading the development of service initiatives. His experience of more than 20 years ranges from strategic business planning to detailed implementation of operations and technology initiatives. Conroy is a frequent speaker on topics ranging from the annual consumer product industry outlook to the American Pantry Study, which takes a deeper look into consumer behaviors and attitudes toward shopping.

Frank Milano

Frank Milano (Deloitte & Touche LLP) is the national leader of the AERS Advisory consumer products sector at Deloitte. In this role, he is responsible for leading client service teams across the sector, including those serving some of the organization's largest multinational clients in the food and beverage, consumer goods, and agribusiness markets. Milano has over 20 years of experience advising clients in the areas of corporate governance, information technology, finance transformation, and supply chain risk, and is a frequent lecturer in these areas.

Anupam Narula

Anupam Narula (Deloitte Services LP) is the research team leader for Deloitte's consumer and industrial products industry practice. He is the research lead and co-author of multiple articles and reports on consumer attitudes and behaviors toward brand loyalty, marketing strategies, and store brands. Narula's published research includes *Digital commerce in the supermarket aisle, Dollar store strategies for national brands, I have not yet begun to shop . . . or have I?, A crisis of the similar*, and *The battle for brands in a world of private labels*.

Raj Singhal

Raj Singhal (Deloitte & Touche LLP) is a senior manager focused on serving global consumer product companies. He specializes in the area of risk management and governance, and has more than 14 years of experience delivering IT- and business-related risk management, program management, and governance services.

Deloitte's consumer products practice helps CPG and other consumer products businesses address issues in areas including consumer behavior and the growth of private label brands, food and product safety, M&A within the industry, supply chain effectiveness, and talent management. We serve companies operating in apparel and footwear, food and beverage/food processing, and personal and household goods. Contact the authors for more information or learn more about our consumer products practice on www.deloitte.com.

Contents

Executive summary: A new perspective on data privacy

DATA privacy and security[1] is about much more than keeping hackers at bay. It is also about assuring consumers that the trust they place in a consumer product brand is warranted. The results of a recent survey of consumers and executives show that consumers have a keen sense of awareness of the risks surrounding data security and privacy, and that many consumer product executives are likely overestimating the extent to which they are meeting consumer expectations related to data privacy and security.[2] On the other hand, many consumer product executives may be underestimating the opportunity for competitive advantage associated with meeting consumer expectations regarding data privacy

ABOUT THE STUDY

The research described in this article encompassed two Web-based surveys conducted in August 2014. One survey polled 70 US consumer product industry executives and senior managers; the other, 2,001 adult US consumers. The research also included six executive interviews conducted in August and September 2014.

Fifty-one percent of the executive survey respondents worked at food products or beverage companies, 34 percent worked at apparel or footwear companies, and the remaining executive respondents worked at household goods or personal care companies. Thirty-nine percent of the executive respondents spent at least 20 percent of their time on activities related to data privacy and security. Forty-four percent were from large companies that recorded annual sales of more than $10 billion a year. Respondent roles and titles reflected a broad range of experience in operations, finance, marketing, information technology, and risk management. A majority of the executives (83 percent) self-reported their company's business performance (e.g., market share, revenue growth, customer loyalty, net profit margin) as higher than or comparable to their competitors during the last three years.

The consumer respondents were screened to target consumers who did at least 25 percent of their household's shopping and had purchased a product online in the past six months. The majority of the consumer respondents (58 percent) were female. Forty-seven percent reported an annual household income of less than $50,000, 32 percent earned between $50,000 and $99,999 annually, and 21 percent earned $100,000 or more annually.

The six executives interviewed had experience with data privacy and security; three of them were IT executives at consumer product companies, two of them were marketing executives with analytics expertise at consumer products companies, and one of them was a mobile application developer with experience working with both retailers and consumer product companies. The interviews covered five topics: responsibility and coordination across the organization for consumer data security and privacy; the level of clarity and understanding across the enterprise of data security and privacy strategy; organizational awareness of regulatory compliance requirements and legal liabilities; the effectiveness of tactics used to manage internal and external threats; and the impact of breaches on the consumers' perception of brands and consumer product companies.

and security. Furthermore, many consumer product companies do not seem positioned to gain consumer trust based on their current data privacy and security strategies, policies, and systems (figure 1). The field appears wide open for consumer product companies to differentiate themselves through a reputation for strong data privacy and security practices. Consumer product executives should consider viewing data privacy and security not just as a risk management issue, but as a potential source of competitive advantage that may be a central component of brand-building and corporate reputation.

Figure 1. Challenge areas related to data privacy and security

	Particularly challenging data privacy and security objectives for many consumer product companies	Typical adherence across the enterprise
Vision and strategy	• Making data privacy and security a critical company-wide priority supported by adequate budget and resources • Maintaining an up-to-date strategy in the event that a breach is identified • Establishing a clear strategy for the collection and use of consumer data	◔
Policies	• Crafting easy-to-understand consumer-facing policies that emphasize opting in instead of opting out • Keeping policies up to date with changing technology and regulations	◔
Organization and people	• Elevating a senior privacy officer to the C-suite with ultimate responsibility for data privacy and security and giving him/her the authority to carry out responsibilities	◔
Processes and systems	• Restricting access to consumer data by business need to know • Tracking and monitoring all access to consumer data • Utilizing advanced cyber techniques (i.e., wargaming) to test security	◑
Risk management	• Identifying potential external and internal threats • Staying up to date on full range of tactics attackers may use • Monitoring third-party providers	◔

Low adherence across the typical enterprise ○ ◔ ◑ ◕ ● High adherence across the typical enterprise

Note: See figure 13 for a more complete list of data privacy and security objectives.

A breach of trust

NEARLY everyone who works in the consumer products industry knows that negative brand experiences can quickly negate years of brand-building, a hard-gained positive reputation, and—perhaps most importantly—the trust a consumer places in a brand.[3] Consider the impact on consumer trust, then, when a company announces that it has experienced a data breach. In this age of big data and digital marketing, in which consumer product companies and retailers are building detailed profiles of individual consumers based on a plethora of data sources, even a single data breach can substantially damage consumer trust. Indeed, 59 percent of consumers state that the knowledge of a data breach at a company would negatively impact their likelihood of buying from that company. Only 51 percent of consumers, moreover, say they would be "forgiving" of a consumer product company that experienced a breach as long as the company quickly addressed the issue.

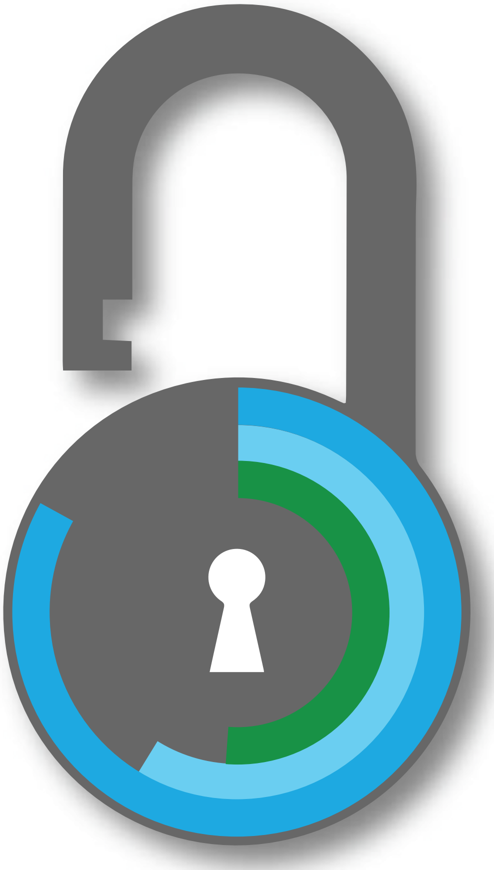
The risk is real—and growing. It is no secret that consumer product companies have been accumulating consumer information with the intent of using big data analytics to improve marketing effectiveness, particularly digital marketing effectiveness. As consumer product companies invest more in targeted digital marketing, the drive to collect consumer information and compile individual consumer profiles is intensifying.[4] The more data a company collects—and the more sensitive that data—the greater the data's attractiveness to malevolent hackers, and the greater the risk associated with data breaches.

Nor are consumers unaware of that risk. Recent data breaches in various industries have heightened consumers' awareness of data security and privacy: 83 percent of the consumers we surveyed were extremely or moderately aware of recent retail breaches. And 83 percent of these same consumers consider security breaches of personal data stored with consumer product companies to be a serious or moderate problem.

Regulators, too, are increasingly aware of the risks to consumer privacy with big data. Edith Ramirez, Federal Trade Commission (FTC) chairwoman, has stated: "Addressing the privacy challenges of big data is first and foremost the responsibility of those collecting and using consumer information. The time has come for businesses to move their data collection and use practices out of the shadows and into the sunlight."[5]

> Recent data breaches in various industries have heightened consumers' awareness of data security and privacy.

Figure 2. Consumers care about data privacy and security



83%

of consumers are aware of recent security breaches of personal data stored with retailers.

59%

of consumers state that a single data breach would negatively impact their likelihood of buying brands from a consumer products company.

51%

of consumers would be forgiving of a consumer product company that had one single data breach of their personal data as long as the company quickly addressed the issue.

Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

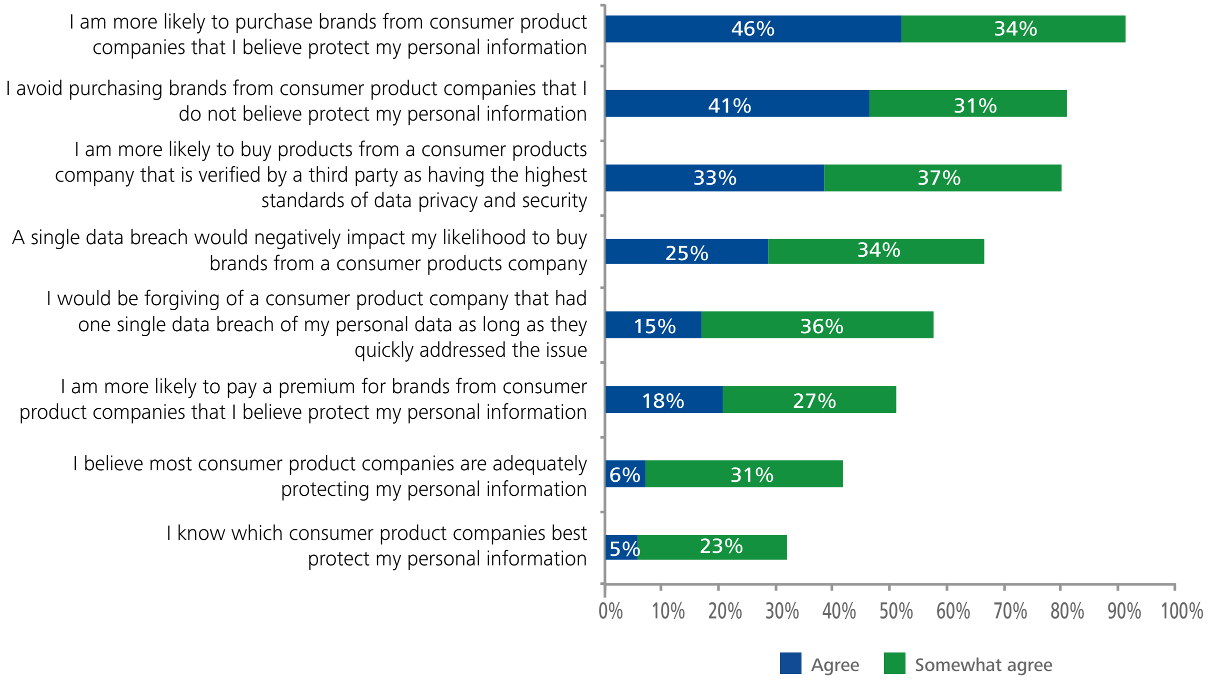
Graphic: Deloitte University Press | DUPress.com

Data privacy and security as a competitive advantage

BUT there is also an upside. There is a clear connection between consumers' perceptions of data privacy and security practices and commercial success. Half of the consumers we surveyed "definitely consider" the privacy and security of their personal information when choosing an online retailer, and 80 percent say they are more likely to purchase from consumer product companies that they believe protect their personal information (figure 3). Furthermore, 70 percent of consumers would be more likely to buy from a consumer product company that was verified by a third party as having the highest standards of data privacy and security. In short, strong data privacy and security practices are not just about risk mitigation, but also a potential source of competitive advantage.

Our survey suggests that the field is wide open for consumer product companies to build a reputation for strong data privacy and security practices. Today, few consumers (37 percent) believe that most consumer product companies are adequately protecting their

Figure 3. Consumers' attitudes and behaviors toward data privacy and security



Source: Consumer responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

personal information. Even fewer consumers (28 percent) think that they know which consumer product companies best protect their personal information. These findings suggest that consumer product companies have yet to establish a name for themselves as trusted stewards of consumer data—and that a company in the industry that can do so can set itself apart from the competition.

LEARNING FROM OTHER INDUSTRIES: WEBMD

WebMD Health Corp. has become a leading provider of health care information for consumers, attracting an average of 138 million unique visitors each month to its public consumer portal, www.WebMD.com.[6] To provide users with tailored health information, WebMD asks them to input data on topics ranging from symptoms to medication to past medical treatments. The site also allows registered users to save their information for later access, in effect creating a record that can be traced back to specific individuals.

How does WebMD get registered users to disclose potentially sensitive health information? A key ingredient seems to be the actions that the company takes to engender user trust. WebMD prominently splashes the logos of third-party privacy and security compliance verifiers, such as TRUSTe, on its website to suggest to consumers that they can entrust their information to the company. Users who register are explicitly informed, up front, about the types of personal information the company might collect about them and that the information will not be shared without permission. Additionally, WebMD maintains a comprehensive and transparent privacy policy that thoroughly details what personal information is being collected from consumers and how it may be used, as well as how the company protects sensitive information.[7] Users see a short summary of the privacy summary at the top of the page, with a link to the full privacy policy underneath; this allows consumers to quickly grasp the privacy policy's highlights without needing to read through the full policy.

After being transparent about how consumer information is collected and used, WebMD puts the ball in the consumers' court to decide what information they wish to disclose, providing the information and tools to allow consumers to either opt out or opt in to sharing their data. Many do choose to share their data, offering up a wealth of personal data that WebMD uses to more effectively tailor its content—and advertisements—to the users' needs.

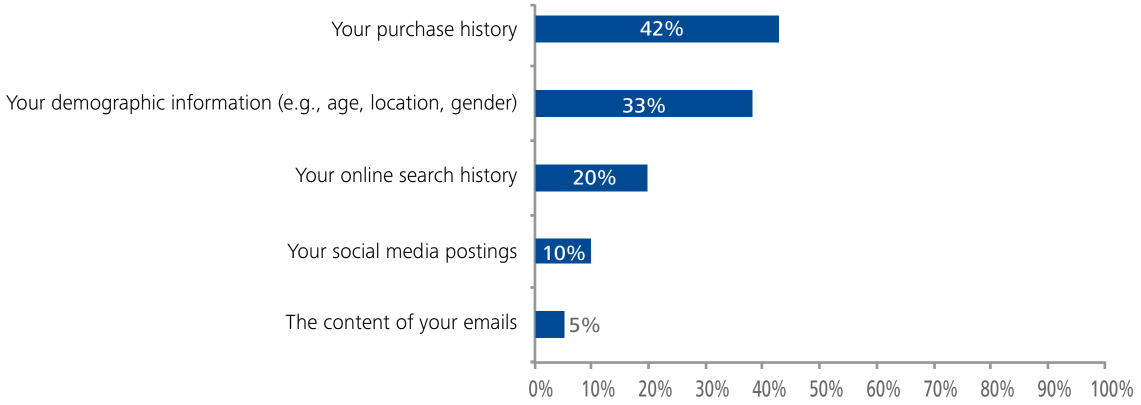
Overestimating consumer comfort

UNFORTUNATELY, convincing consumers to trust consumer products companies with their personal information may be something of an uphill battle. Our research revealed a certain degree of consumer skepticism, even cynicism, about corporate motives and practices around the collection and use of personal data. In the words of one consumer we interviewed: "It would be hard for me to feel reassured that big companies are protecting my interests as it relates to the privacy and security of my personal information. I'm more inclined to think that companies are so concerned with wringing as much potential as they can from a consumer that they don't really care about how consumers feel."

In general, consumers are hesitant to knowingly allow consumer products companies to use their personal information for targeted marketing. While nearly half (42 percent) are willing to allow their purchase history to be analyzed, the vast majority do not believe that their demographics, social media postings, online search history, or emails should be analyzed by software programs (figure 4)—all of which are common practice today in digital advertising placement.

Furthermore, our results suggest that many consumer product executives may not be fully aware of how much ground needs to be gained in the quest for consumer trust around data privacy and security. Fifty percent of the executives we surveyed thought that many consumer product companies are "adequately" protecting consumer information; only 37 percent of the consumers we surveyed thought the same (figure 5). Many executives also seem to be more complacent about their companies' data privacy and security policies than consumers' opinions warrant. While 77 percent of the executives in our study believed that their employer had clear and well-understood

Figure 4. Which of the following should consumer product companies be able to analyze using software programs in order to send targeted advertisements or coupons? Select all that apply.



Note: Figures indicate the percentage of consumers selecting each option.

Source: Consumer responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

CONSUMER CONCERNS ABOUT CONSUMER PRODUCT COMPANIES' DATA PRACTICES

Consumers may appreciate the benefits of personalization and customization, but many are still wary of the extent to which their data can be monitored and recorded. Among the consumers we surveyed:

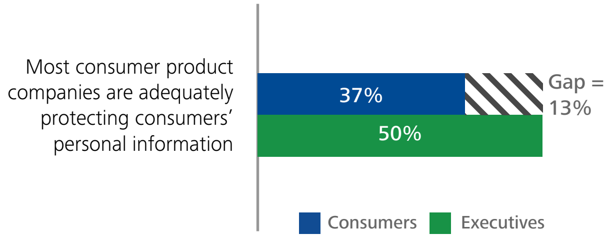
- 85 percent said that they were concerned about consumer product companies tracking mobile phone behavior
- 81 percent were concerned consumer product companies tracking their online behavior
- 78 percent were concerned about sharing their personal data with consumer product companies
- 69 percent were concerned about product companies using online behavior to make product recommendations

consumer data privacy policies, many of the consumers we surveyed sought easier-to-understand policies ("Write the policies in clear and readable English," said one consumer, "and in print large enough to read"). And of the consumers we surveyed who said that they either "carefully read" or "skim" privacy policies, nearly two in five reported deciding not to purchase from an online retailer as a result of its privacy protection policies.

Interestingly, our research hints that consumer product executives may be overestimating, not just consumers' comfort with sharing their personal data, but also the extent to which they feel they receive fair value in exchange (figure 6). Specifically, while 47 percent of the executives we surveyed felt that consumers believe that the risks of sharing personal information are worth the personalized promotions, advertising, or coupons they receive, only 25 percent of the surveyed consumers agreed. Similarly, 47 percent of the surveyed executives thought that consumers believe that the risks of sharing personal information are worth the product recommendations they receive; only 18 percent of the surveyed consumers thought the same.

Consumers are also more likely than executives to hold consumer product companies responsible for data privacy and security (figure 7). When asked who they thought should be responsible for ensuring consumer data privacy and security, 81 percent of consumers said that they believed that consumer product companies were mostly or completely responsible, compared with only 63 percent of executives

Figure 5. Consumer vs. executive perspectives on how consumer product companies are currently protecting consumers' personal data

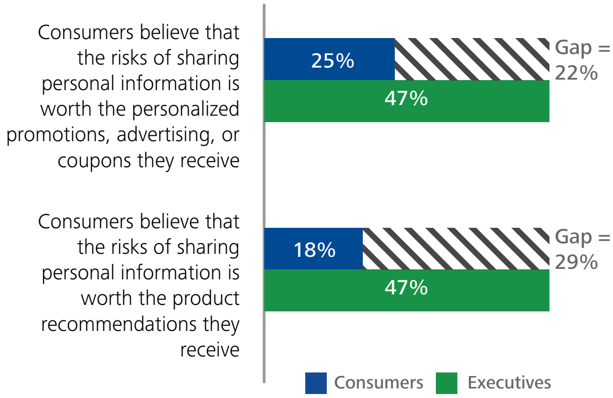


Note: Figures represent the proportion of respondents who agreed or somewhat agreed with the statement.

Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

Figure 6. Personalized offers or recommendations do not outweigh the perceived risks of sharing information

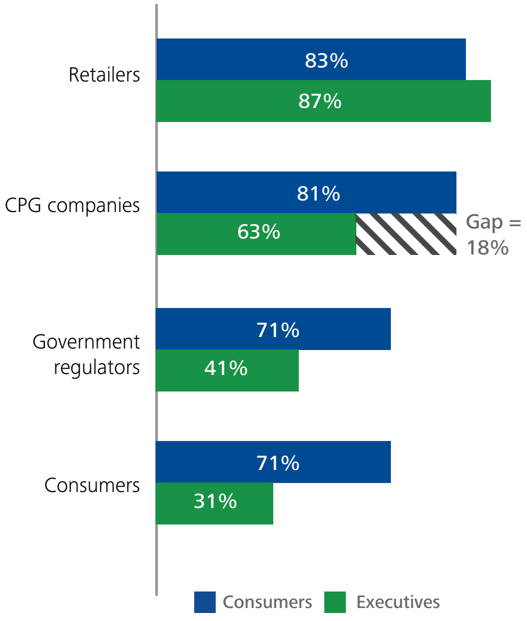


Note: Figures represent the proportion of respondents who agreed or somewhat agreed with the statement.

Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

Figure 7. To what level are the following constituents legally responsible for ensuring consumer data privacy and security?



Note: Figures represent the proportion of respondents who selected "completely responsible" or "mostly responsible" for each constituent.

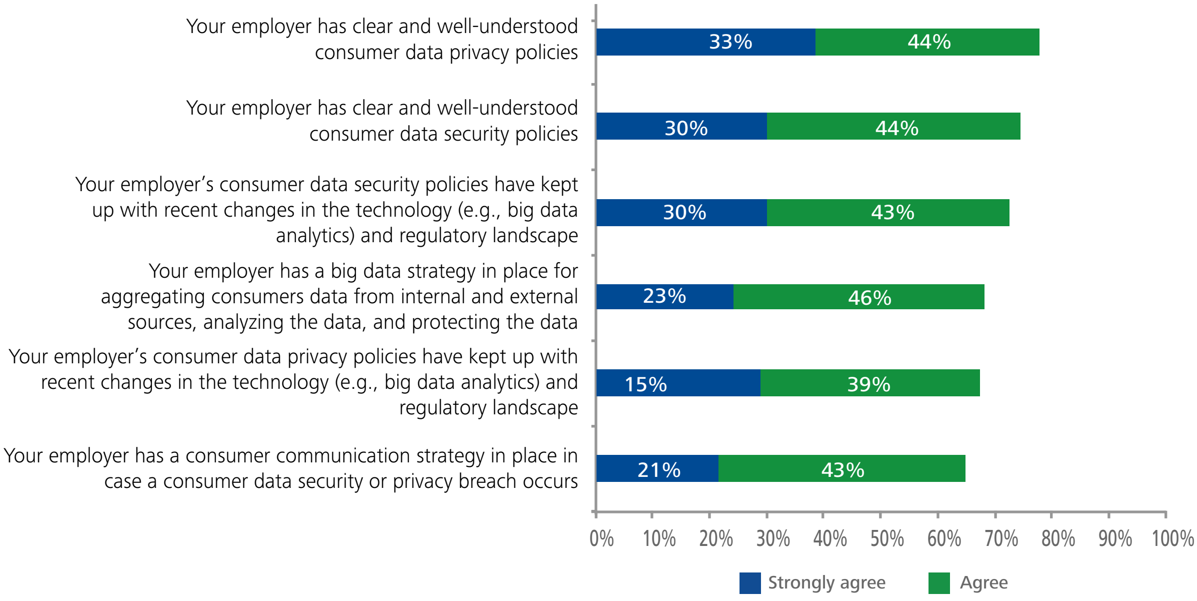
Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

who felt that consumer product companies were mostly or completely responsible.

All this being said, the tendency to overestimate consumer comfort with consumer product companies' data privacy and security practices does not mean that executives are blind to the risks. Reputational damage to brand, loss of current consumers, loss of potential new consumers, and lawsuits from consumers topped the list of risks executives cited with regard to data privacy and security.[8] Moreover, many of the executives in our study were less than completely confident in their own companies' data privacy and security practices. Only 41 percent of the surveyed executives stated that consumer data privacy was "absolutely critical" at their employer; only 37 percent stated that consumer data security was "absolutely critical."[9] Fewer than one-third of the executives surveyed "strongly agreed" that their company's privacy and security policies had kept up with recent technology and regulatory changes or that their company had a consumer communication strategy in place if a breach occurred (figure 8).

Figure 8. Executives' perspectives on consumer data privacy and security policies and strategies



Source: Executive responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

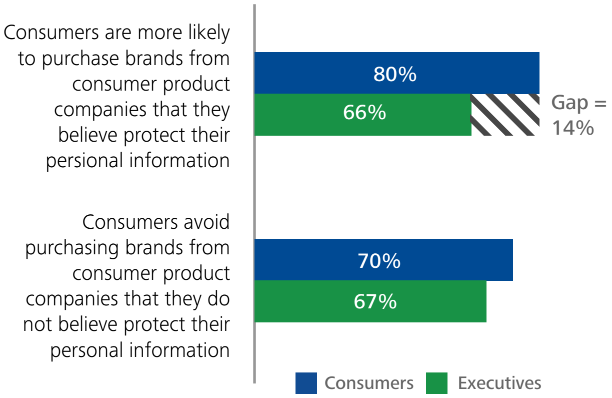
Graphic: Deloitte University Press | DUPress.com

Underestimating the competitive opportunity

THE good news is that consumer product companies could stand to gain a great deal from strengthening their privacy and security practices—and communicating these strong practices to consumers. In particular, the link between purchase decisions and perceived data security is stronger than many executives believe. Sixty-six percent of the executives in our survey thought that consumers are more likely to purchase brands from consumer product companies that are perceived to be protecting their personal information—but the actual proportion of consumers who agreed with this statement was much higher, at 80 percent. Similarly, the proportion of consumers who agreed that they would avoid purchasing brands from consumer product companies that are not perceived to be protecting personal information was somewhat higher than the proportion of executives who agreed with this statement (figure 9).

> The link between purchase decisions and perceived data security is stronger than many executives believe.

Figure 9. Link between perceived data protection and consumer purchases

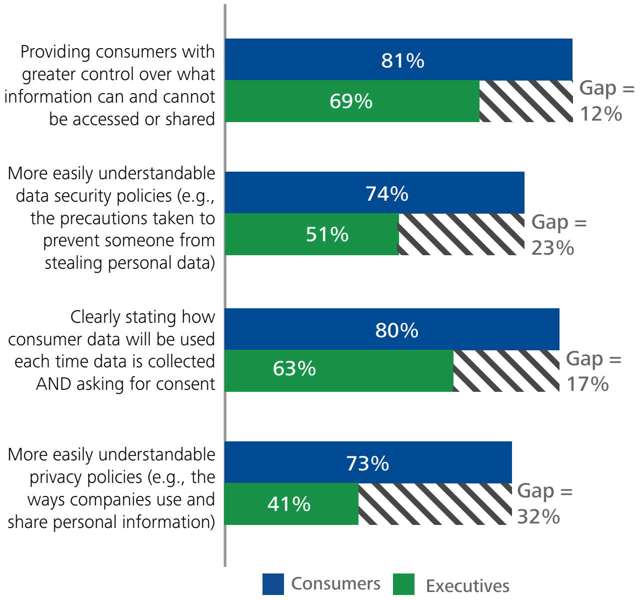


Note: Figures represent the proportion of respondents who agreed or somewhat agreed with the statement.

Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

Figure 10. Which of the following steps would increase your trust in consumer product companies in protecting your personal information related to your online behavior? Select all that apply.



Note: Figures represent the proportion of respondents who selected each option.

Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

Consumers also appear more amenable to being influenced by clarity and transparency around corporate data privacy and security practices, as well as by the ability to control how their data is used, than executives may suppose. For each of four possible actions we described in our survey, a higher proportion of consumers than executives indicated that the action would help "increase trust" in a company's data privacy and security practices (figure 10). Especially worth noting is the importance consumers place on a company's privacy policy—even though many admit to only "skimming" privacy policies when purchasing product online as opposed to "carefully reading" them (figure 11). Seventy-three percent of our surveyed consumers agreed that easy-to-understand privacy policies would increase their trust in consumer products companies with regard to the protection of their personal information.

Figure 11. Most consumers only skim consumer privacy protection policies

Survey question: To what extent do you read consumer privacy protection policies when …

	Full extent (e.g., read completely)	Low extent (e.g., skim quickly)	Don't read at all or unaware of privacy policy
Purchasing product online	13%	73%	14%
Using social media (among social media users)	17%	58%	25%
Using search engine	11%	48%	41%
Using email service	13%	50%	37%

Source: Consumer responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

THE DRIVE FOR BIG DATA ANALYTICS

As many consumer product companies begin to build big data repositories and analytics capabilities, many are eagerly exploring the art of the possible with consumer data gathered from product registrations, social media, direct-to-consumer e-commerce programs, loyalty programs, and retailers.[10] Many of the executives in our survey indicated that their companies are using data analytics to support marketing programs such as targeted marketing via online, mobile, and social media channels; many also believe that these programs have been effective in driving increased sales (figure 12).

Figure 12. Data analytics has increased sales at many consumer product companies

	Percentage of companies conducting this type of data analytics with consumer data	Effectiveness of data analytic efforts in driving increased sales*
Targeted marketing via online/mobile advertisements	71%	82%
Loyalty programs	67%	81%
Input to new product development	57%	80%
Targeted marketing via social media	69%	79%
Targeted marketing via online/mobile coupons	71%	79%
Trade promotion optimization	49%	76%
Targeted direct mail campaigns	66%	76%
Modeling of consumer segment behavior	57%	75%
Collaborating with retailers on retailer-specific promotions	60%	72%
Third-party retail transaction data	47%	66%

* The figures in this column reflect the percentage of executives who said that each tactic was effective or somewhat effective in increasing sales.

Source: Executive responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Five considerations for stronger data privacy and security practices

BECAUSE gaining consumer trust around data privacy and security can translate into competitive advantage, consumer product companies should consider treating data privacy and security not just as a risk management issue, but as a central component of brand-building and corporate reputation. To strengthen both the reality and the perception of corporate data privacy and security practices, we suggest that consumer product companies consider objectives in five areas (figure 13).

1. Take on the consumer mindset in setting the vision and strategy for what data is collected, how data is analyzed and used, and how breaches are handled.

"Provide clear and frequent updates on what personal information is held and how and when the information is provided to others."
—Consumer survey respondent

"Be as clear and transparent as possible with consumers, and then follow through with strict data policies."—Executive survey respondent

Taking the consumer mindset is an important part of building a brand for strong data privacy and security practices. By "taking the consumer mindset," we mean developing a vision and strategy for using and protecting consumer data with an acute awareness of how consumers might interpret the company's activities. Leaders should consider understanding what consumers appreciate and what they might object to in the use of their personal data, and examine both their goals and their tactics with the consumer perspective in mind. Questions to ask may include:

- How do we aim to improve the consumer experience, from awareness and consideration to initial product trial and repeat purchase?
- What data do we have or need to collect to improve the consumer experience at each of these steps?
- In what situations (e.g., for what types of data or what types of analyses) should we seek consumer consent or allow them to opt in, as opposed to defaulting to collecting/using their data?
- How do we avoid collecting or storing "excess" consumer data that we do not use or do not need? If we have excess data that could be harmful to consumers if breached, what do we do about it?
- Which of our attempts to improve the consumer experience could be viewed as "creepy" or intrusive instead of helpful?
- How transparent, timely, coordinated, and comprehensive are we if or when there is a breach?

Many consumers may share the perspective of one consumer we surveyed, who implored

Figure 13. Examples of consumer product company data privacy and security objectives

Area	Objectives	Level of adherence across the typical multi-national consumer product company[11]	Level of difficulty in deploying across the organization	Possible sequence of deploying advanced adherence
Vision and strategy	Making data privacy and security a critical company-wide priority supported by adequate budget and resources	◔	Low	Wave 1
	Maintain an up-to-date strategy in the event that a breach is identified*	◔	High	Wave 1
	Establish a clear strategy for the collection and use of consumer data*	◔	High	Wave 1
Policies	Establish clear internal data use and retention guidelines understood across the organization	◑	Moderate	Wave 2
	Keep policies up to date with changing technology and regulations*	◔	Moderate	Wave 2
	Craft easy-to-understand consumer-facing policies*	○	Moderate	Wave 2
Organization and people	Elevate the seniority of the executive with ultimate responsibility for data privacy and security*	◔	Moderate	Wave 1
Processes and systems	Maintain secure firewall configuration	◑	Low	Wave 3
	Assign a unique ID to each person with computer access	◕	Low	Wave 1
	Use and regularly update anti-virus software	◕	Low	Wave 1
	Encrypt customer data when transmitting	◑	High	Wave 3
	Restrict access to consumer data by business need to know	◔	High	Wave 3
	Track and monitor all access to consumer data	○	High	Wave 3
	Utilize advanced cyber techniques (i.e., wargaming) to test security	○	High	Wave 3
Risk management	Identify potential external and internal threat actors and risk profiles	◔	High	Wave 1
	Understand the company's data targets and their potential attractiveness to attackers	◔	High	Wave 2
	Stay up to date on the full range of tactics attackers may use	◑	High	Wave 2
	Identify, monitor, and audit third-party providers	◔	High	Wave 2
	Regularly test security systems and processes	◑	High	Wave 2

* Related to consumer perceptions of trust

Low adherence across the typical enterprise ○ ◔ ◑ ◕ ● High adherence across the typical enterprise consumer product companies to "ask for my consent and allow me to decide which information I want to share." While transitioning to a world of "opting in" rather than "opting out" may reduce digital marketing ROI in the short term, it can pay off in the long term in the form of greater trust and greater consumer openness to sharing data. "Consumers are more willing to share personal information if they know the rules, and raise their hand to opt in," according to one mobile consumer tool developer we interviewed.[12]

To better understand the consumer perspective on these and similar matters, it can be useful to segment consumers based on their awareness of and level of concern with data privacy and security issues. A prudent approach could be to develop a vision and strategy based on the views of the consumer segment that is *most* aware of and concerned with data privacy and security. A company that meets the needs of these discerning consumers will likely exceed the needs of the others.

2. Develop privacy policies as if they were a marketing tool rather than only a legal disclosure.

"Companies should have simplified privacy policies. Now you have to practically have a law degree to understand them."—Consumer survey respondent

A privacy policy's goal should not only strive to inform consumers of the precautions a company has in place around data protection and use, but also—and just as importantly—aim to increase the willingness of consumers to share their personal data. Leaders should view their company's privacy policy as a strategic communication that, by making a commitment to consumers to safeguard their personal information, maintains and even builds trust. However, few companies appear to see their privacy policy as anything more than a legal safeguard. A privacy policy over a dozen pages long, written in arcane legal language, and presented in a tiny font size does not likely inspire a great deal of trust, particularly when it is difficult for consumers to find.

According to our research, two of the most important ways that consumer product companies can increase trust in their data privacy and security practices are by clearly stating how consumers' personal data will be used and by giving consumers more control over the use of their data. A privacy policy should therefore lead with easy-to-understand language that addresses these fundamental issues. Points to cover include:

- What personal data does the company collect?
- How does the company use the data?
- How does the company protect the data?
- How do consumers opt in and opt out of the collection or use of their data?
- How do consumers benefit from the collection and analysis of their data?

One tactic for shortening and simplifying the privacy policy is to present key information in plain English on the main privacy policy page, then provide links to more comprehensive details for those consumers interested in the fine print. Recall that many consumers skim, rather than carefully read, privacy policies—making it essential for companies to get the main messages across quickly and simply.

To back up the promises made by the privacy policy, companies should consider developing clear internal data use and retention guidelines across the organization that directly link to the consumer privacy policy. These guidelines could drive behavior both within the company's own organization and at its partners. And, given the ever-changing technological and regulatory landscape, it is important to regularly revisit policies to keep them up to date.

LESSONS FROM OTHER INDUSTRIES: AMERICAN EXPRESS

With more than 107 million card-carrying customers,[13] American Express (AMEX), one of the largest US bank card issuers, is responsible for the daunting task of safeguarding the privacy and security of the data it collects from its card-holding members. Consumers seem to think that AMEX is doing a good job. The company earned the top spot among financial services companies in the annual Most Trusted Companies for Privacy Study by Ponemon Institute, a ranking of companies consumers most trust to protect the privacy of their personal information, from 2007 to the most recent report in 2012.[14]

The way AMEX responded to one industry data breach illustrates how a focus on consumer privacy protection and security preparedness can help build consumer trust. On September 7, 2000, a company press release announced a new suite of tools developed to safeguard members' privacy when shopping online.[15] The very next day, another financial services company reported that hackers had gained access to more than 15,000 card numbers and related customer information.[16]

In the wake of the hack, bank card industry players were called upon to provide solutions to protect online consumer privacy and security. AMEX had done its homework, and was prepared to respond to this need both independently and in tandem with others. Its actions included joining forces with peers to create the Worldwide E-Commerce Fraud Prevention Network.[17] Analysts noted AMEX's preemptive preparedness and how well the company worked with others during the crisis[18]—actions that helped burnish its image as a privacy leader.

3. Elevate the seniority of the executive with ultimate responsibility for data privacy and security.

"Responsibility [for data privacy and security] doesn't roll up to one place at many consumer product companies due to their size and complexity. A corporate privacy officer's role should be to set overall company policy and ensure that the policy is adequately deployed in the organization. However, to do this, the privacy officer has to have the budgetary authority and the managerial control to enforce company policy."—Consumer products information technology executive interviewee

It is our view that large consumer product companies looking to reassure consumers of the precautions in place around data privacy and security—as well as ensure compliance with data privacy and security laws across a multinational enterprise—should consider having a senior privacy officer (e.g., chief privacy officer) who reports directly to the CEO. As one executive interviewee pointed out, a privacy officer's responsibilities require a certain amount of authority and budget to carry out. A privacy officer considered a peer to the chief marketing officer, chief information officer, and general counsel is more likely to be able to effectively carry out those responsibilities, which may include weighing the trade-offs between business needs (e.g., targeted promotional campaigns based on personal data) and technology precautions; advocating on behalf of the consumer; and providing the consumer perspective to help determine what level of risk and exposure is acceptable to the company. Optics are also important: A company that puts its top privacy officer in the C-suite sends a message to the marketplace that it takes protecting consumer data seriously.

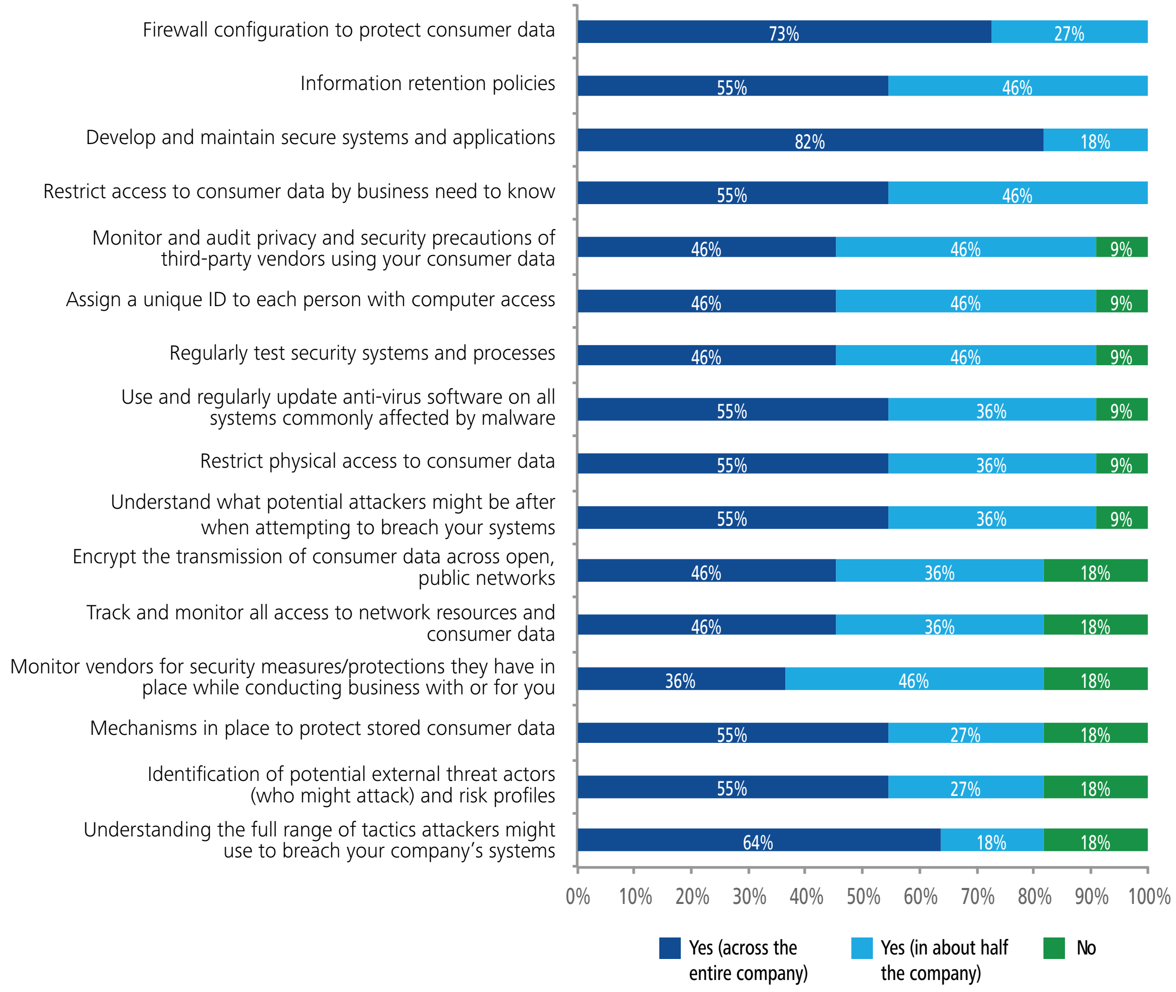
For many consumer product companies, having a privacy officer in the C-suite rather than within the information technology department would likely be a change. Only 41 percent of the executives we surveyed worked at a company where the leader ultimately responsible for consumer data privacy reported directly to the CEO. Even fewer executives (34 percent) worked at companies where the leader of consumer data security reported directly to the CEO.

4. Deploy supporting processes and systems consistently across the enterprise to reduce exposure and mitigate threats.

"Stay current on threats and continuously upgrade technology."—Executive survey respondent

If personal data is compromised or misused, consumers are unlikely to care which department's or division's fault it is. Consequently, all parts of the enterprise must have processes and systems in place to safeguard data privacy and security and to mitigate threats. Unfortunately, deploying processes and systems across a complex organization is often challenging, as many disparate data repositories often exist. When asked about the extent to which their companies had deployed a variety of process and system capabilities for protecting consumer information, the percentage of executives who reported that their organization had deployed a capability "across the entire company" ranged from a high of 82 percent (for developing and maintaining secure applications) to a low of just 36 percent (for monitoring vendors' security practices) (figure 14). These results suggest that many consumer product companies do not have many basic data privacy and security tactics in place across the entire enterprise.

Figure 14. Executives' views on the extent to which their company has implemented capabilities to protect consumer data privacy and security



Source: Executive responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Graphic: Deloitte University Press | DUPress.com

Our executive interviews revealed a number of approaches to achieving organization-wide consistency in data privacy and security practices. One consumer product information technology executive emphasized the importance of reducing exposure to simplify the deployment of processes and systems. This executive's company systematically inventories areas of exposure and then examines whether these areas could be removed as exposures—for instance, by shortening the data retention period or by not collecting certain data elements. This approach reduces the extent to which processes and systems to safeguard data are required in the first place, thereby easing the challenge of deploying them across the organization.

Top-down governance can also be useful in achieving consistent deployment, as demonstrated by one multinational, multi-product-line consumer product company that maintains a privacy council that supports the senior privacy officer. Through the council, accountability for privacy is consistently deployed across the organization to key business units responsible for the communication of privacy standards to employees. The council also oversees compliance with global privacy standards, and sees that consistent privacy policies are instituted and maintained across all data types and countries.

5. Expand risk management around data privacy and security to guard against not just external malicious breaches, but also inadvertent internal breaches and third-party partner breaches.

"Consumer product companies should not assume that adequate privacy and security precautions are in place with digital marketing vendors. They should be verifying with third-party audits."—Consumer product information technology executive

Malicious hackers aren't the only source of data security risk. A company's own employees often have opportunities to compromise data security, either inadvertently or intentionally. Further, for many targeted marketing campaigns, much of the actual work is done by third parties—vendors and contractors with whom a company must share consumers' personal data. It is therefore imperative to consider expanding risk management to install safeguards against both third-party partner breaches and internal security lapses, as well as against external threats. Steps to consider include:

> Our executive interviews revealed a number of approaches to achieving organization-wide consistency in data privacy and security practices.

- Identify potential external and internal threat actors and risk profiles. This allows companies to step into the shoes of potential security threat actors to better characterize the precautions required.

- Understand the company's data targets and their relative attractiveness to attackers. Creating a tiered policy that prioritizes the level and number of privacy and security controls in place can be a good starting point.

- Stay up to date on the full range of tactics attackers may use. Expect attackers to be creative and breaches to occur, and plan to have multiple layers of protection to render some breaches "harmless."

- Identify, monitor, and audit third-party providers. Don't assume vendors are complying with the data privacy and security stipulations in work agreements. Confirm that they are complying, and identify and address weaknesses in their systems and processes.

- Regularly test security systems and processes. As consumer product companies continue to link previously separate data sources to create a single view of the consumer, they may inadvertently create privacy and security lapses. Regular testing increases the probability of companies identifying issues before attackers do.

- Simulate cyber attack scenarios to evaluate incident response preparedness and identify response deficiencies. Cyber wargaming can allow companies to develop a shared perception of cyber security threats. Consumer product companies that understand key dependencies and inventory sources of consumer information prior to a cybersecurity incident are better positioned to respond. They should stress test the communication of strategic and technical information between executive management and IT team.

As one consumer we surveyed said, "I'm not sure that there is anything that companies can do [about hackers]. Hackers will always be finding new ways to access information." However, it is possible that, while consumers may perceive external threats as more or less inevitable, internal threats and third-party breaches may be seen as more avoidable—and therefore less forgivable. If this is the case, then it becomes especially important for consumer product companies to consider safeguarding data privacy and security in areas over which they have some measure of control.

A matter of trust

WHEN it comes to consumer privacy, begin and end with the mantra of "build consumer trust." It is easy to understand consumers' hesitation about having their often private preferences—for products, brands, and media—and their social media activities aggregated and analyzed to uncover the essence of their shopping behaviors. Cultivating positive consumer perceptions of data privacy and security practices can help offset this unease, and thus become a potential source of competitive advantage. Rather than forego the unequivocal value of gathering and using personal consumer data to drive targeted digital marketing, consumer product companies can seize the opportunity to build brand trust by meeting—and even exceeding—consumer expectations related to data privacy and security.

Appendix: A deeper look at the consumer perspective

WHAT can retailers and consumer product companies do to reassure consumers that they are protecting the privacy and security of their personal information? When we asked consumers in our survey this question, the answers appear to cluster around six themes (figure 15):

- Provide transparency in policies and actions
- Be judicious about collecting and sharing data
- Inform and reassure customers about security measures
- Protect consumers
- Be prepared to compensate for security lapses
- If there is a breach, regain consumers’ trust

Figure 15. Reassuring consumers that their personal information is being protected

Theme	Consumer quotes
Provide transparency in policies and actions	• “Write the policies in clear and readable English and in print large enough to read.” • “Provide clear and frequent updates on what personal information is held and how and when the information is provided to others.” • “Companies should have simplified privacy policies. Now you have to practically have a law degree to understand them.”
Be judicious about collecting and sharing data	• “Collect the least amount of info necessary and give every clearly stated opportunity to opt out of stating personal info.” • Don’t sell my information to third parties, ask for my consent, and allow me to decide which information I want to share.” • Refrain from spamming or overuse of marketing awareness. I am less likely to buy if I feel my information is being taken advantage of or sold.”
Inform and reassure customers about security measures	• “Send periodic emails regarding how they protect my privacy and security to give me more assurance.” • “Respond quickly when a breach is detected. A third party verification [of security measures] would be helpful.” • “First, have a good record. Second, tell me what you are doing to protect my personal information.”
Protect consumers	• “Test systems more often for holes and have security measures in place that prevent hacking.” • “Be a LOT more vigilant.” • “Use better encryption and keep personal data in secure and constantly monitored facilities.” • “Run security audits on systems.”
Be prepared to compensate for security lapses	• Should fraud happen, I should be reimbursed for what was spent on my credit cards.” • “Offer to compensate consumers for their time and trouble if a security breach occurs. Have [companies] put their money where their mouth is.” • “Insist on stiffer penalties for those who cause security breaches.
If there is a breach, regain consumers’ trust	• “Stand behind the security policy in place.” • “Actually do something and not just talk about improving.” • “Actually care and follow through with it. Humans are more than just data.”

Source: Consumer responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

Endnotes

1. In this report, we use "privacy" to refer to precautions companies take in the ways they use and share consumer data, and "security" to refer to the precautions companies take to prevent others from stealing consumer data.
2. Unless otherwise stated, all statements in this report on consumer and executive opinions are taken from data collected in an August 2014 consumer product consumer and executive survey on data privacy and security conducted by Deloitte LLP. Details on the survey are described in the sidebar titled "About the study" in this document.
3. According to Deloitte's *2014 American pantry study*, consumers describe three-quarters of the brands in their shopping cart as brands they trust. Furthermore, the leading reason consumers say they purchase higher-priced products when cheaper alternatives available is that the "product is by a brand I trust." See *The 2014 American pantry study*, Deloitte Development LLC, 2014, http://www.deloitte.com/view/en_US/us/Industries/consumer-products/56f2c1ae91da5410VgnVCM3000003456f70aRCRD.htm#.VCmK_fldWSo.
4. Pat Conroy, Rich Nanda, and Anupam Narula, *Digital commerce in the supermarket aisle: Strategies for CPG brands*, Deloitte University Press, December 13, 2013, http://dupress.com/articles/supermarket-digital-commerce-cpg-strategies/.
5. Edith Ramirez, chairwoman of the Federal Trade Commission, "The privacy challenges of big data: A view from the lifeguard's chair" (keynote address, Technology Policy Institute Aspen Forum, Aspen, Colorado, August 19, 2013).
6. WebMD Health Corp., Form 10-K, annual report filed with the SEC on March 3, 2014.
7. WebMD Health Corp., "WebMD privacy policy summary," http://www.webmd.com/about-webmd-policies/about-privacy-policy, accessed April 10, 2014.
8. Executive survey question: "Please rank order the top five impacts of a data breach to a consumer product company."
9. Executive survey question: "How important is consumer data security at your employer?"
10. Conroy, Nanda, and Narula, *Digital commerce in the supermarket aisle*.
11. The assessment of typical consumer products companies' level of adherence is based on project experience with 12 clients in 2013 and 2014, executive survey, and executive interviews.
12. Jamie Thompson, Sprinklenet Labs, interview with the authors, September, 3, 2014.
13. American Express, "Welcome to American Express," http://about.americanexpress.com/, accessed September 29, 2014. Data were current as of December 30, 2013.
14. Ponemon Institute, *2012 most trusted companies for privacy*, January 28, 2013, http://www.ponemon.org/blog/2012-most-trusted-companies-for-privacy.
15. Ibid.
16. Associated Press Newswire, "Western Union Web site hacked; credit cards number taken," September 10, 2000.
17. PR Newswire, "Together to fight fraud: American Express, buy.com, ClearCommerce, Expedia.com, First Data, Paymentech, Starwood Hotels & Resorts Worldwide and Ventro Corporation form first merchant-driven effort to share best practices," September 25, 2000.
18. Network World Fusion, "Credit card companies introduce new security," September 18, 2000.

Acknowledgements

The authors would like to thank **Julie Finn** (Deloitte Services LP), **Junko Kaji** (Deloitte Services LP), **Robert Libbey** (Deloitte Services LP), and **Anup Raju** (Deloitte Support Services India Pvt. Ltd) for their significant contributions to the research and writing. We would also like to acknowledge the contributions of **Sushant Gaonkar**, **Shweta Joshi**, **Vaibhav Khobragade**, and **Neelakantan Subramanian** (all of Deloitte Support Services India Pvt. Ltd).

Contacts

Pat Conroy
Vice Chairman and US Consumer Products leader
Principal
Deloitte LLP
+1 317 656 2400
pconroy@deloitte.com

Frank Milano
US Consumer Products Audit and Enterprise Risk Services Advisory leader
Partner
Deloitte & Touche LLP
+ 1 917 656 2093
fmilano@deloitte.com

Deloitte
University
Press

Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press

Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.