Bridging the trust divide

Consumers see little difference between data privacy and security, says Brunswick Insight's PETER ZYSK

Your company might have a cybersecurity officer and a privacy officer, with separate responsibilities. The problem is, your customers don't think that way.

New research from Brunswick Insight finds that consumers around the world rarely distinguish between data privacy and data security. While data is becoming increasingly important to companies, consumers are expressing a growing fear of data theft and a deepening skepticism about how their personal information is collected and protected.

As a result, they are beginning to withhold information, exhibiting newfound caution. A US Department of Commerce study found that privacy and security concerns stopped nearly half (45 percent) of US households on occasion from some online action such as shopping, banking or social activities.

Our survey of more than 7,000 consumers across Asia, Europe and the Americas shows that clear communication about data protection policies can go a long way toward easing consumers' security concerns. Consumers know that their personal data is constantly being collected and they recognize that their online privacy may be diminished as a result. In the survey, the most frequently used term selected to describe company data collection practices is "intrusive."

This response is not just simple irritation, but downright fear – so much fear, in fact, that in many countries concerns about the security and privacy of personal data top those about the economy, war, healthcare or climate change. Consumers are three times more likely to be afraid of how companies may use their data than excited about the potential for innovation and advancement. Companies clearly need to do more to communicate the benefits of data collection.

As a group, organizations that collect data receive little benefit of the doubt. Nearly two-thirds of consumers (62 percent) believe companies should do more to protect personal information, and nearly half (43 percent) say they trust companies with their data less than a year ago. This finding is consistent worldwide.

> **"Remember: when you say "privacy," consumers hear "security"**"

The research also shows consumers consider a company's privacy policy in the context of their security concerns, heedless of the distinction companies draw between privacy and security. Companies may claim to use only "aggregate" or "anonymous" data, but those terms fall on deaf ears, failing to specifically address customers' concerns about data theft.

There are three things companies can do to better meet consumer expectations:

Use a cross-functional team To create an integrated data narrative, you need to involve wide representation from across the company.

Keep security front and center Your safeguards are a critical part of your message. And remember: when you say "privacy," consumers hear "security."

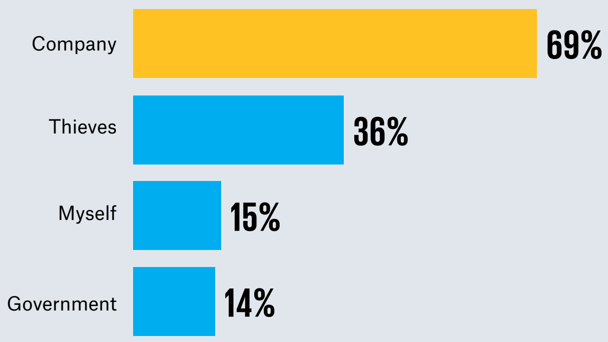
Prepare When bad things happen in the cyber realm, companies have to assume they will be blamed. Prepare now, to reduce the potential reputational harm.

PETER ZYSK is an Associate in Brunswick Insight's opinion research practice and is currently based in Beijing.

ACCOUNTABILITY

IN A BREACH, WHO WOULD YOU BLAME?

Who would you blame if a business you use was hacked, and your personal information stolen?



Percentages do not total 100, due to multiple response options

Consumers hold companies to a high standard when it comes to protecting their personal data. Even if a hacker were responsible for the loss of consumer data, consumers would blame the company. In addition, most consumers said they would stop buying from the company and encourage others to do the same (see "Ready to boycott," Page 13)

▶ **Data security and privacy top the list of consumer concerns in five out of seven countries surveyed. Exceptions include the US, where the top economy is the top worry, and Germany, where the chief fear is terrorism**

RANKING THREATS

HOW CONCERNED ARE YOU ABOUT...

Security of my personal data	Privacy of my personal data	State of the economy	Terrorism or war	Access to healthcare	Climate change	Security of my job
87%	86%	80%	76%	74%	73%	58%

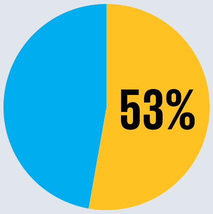
Data combines those that selected “very concerned” and “somewhat concerned”

▶ **Corporations can do a better job of explaining how they protect personal information. It seems clear that when companies say “data privacy,” consumers hear “data security.” A majority of consumers in our survey selected a security-centric definition of data privacy**

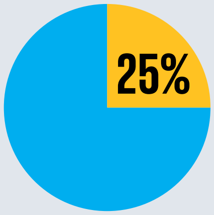
DEFINITION OF TERMS

PRIVACY AND SECURITY ARE BLURRED

How do you define data privacy?



Collected data will not be used or accessed by **unauthorized individuals or parties**



Collected data will only be used for **agreed purposes**

Participants were asked to select the description that best describes data privacy. The two shown here ranked highest

In a separate question about data privacy concerns (how companies use the data they collect), the theft of personal information was the overriding concern of more than 64 percent of respondents – double the number worried about the improper sharing of information

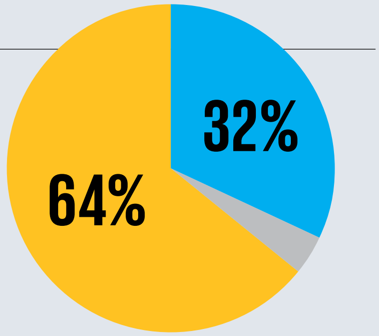
SECURITY IS THE TOP CONCERN

What is your main data privacy concern?

🟨 I am most concerned about my personal information being **stolen by hackers** or compromised in any other way that could make me a victim of identity theft

🟦 I am most concerned about companies recording my physical location or online activity and then **selling or sharing** this information with other companies

⬜ Unsure



BRUNSWICK INSIGHT

Brunswick Insight provides critical issues research for market-moving decisions, and combines experienced, data-driven counsel with an emphasis on rapid research and analysis. Insight converts research into strategic advice for communications programs and campaigns

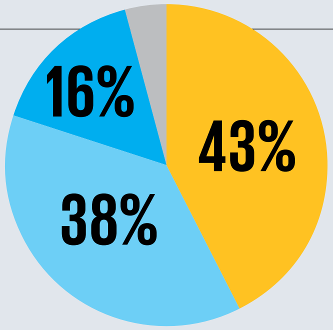
This research is based on a February 2016 Brunswick Insight survey of 7,029 consumers in Brazil, China, France, Germany, Singapore, the United Kingdom and the United States. A nationally representative sample of around 1,000 consumers was surveyed in each country

TRUST

BREACHES ARE A TEST OF FAITH

How much do you trust companies to keep your data secure, compared to a year ago?

🟨 Trust less
🟦 Trust the same amount
🟦 Trust more
⬜ Unsure

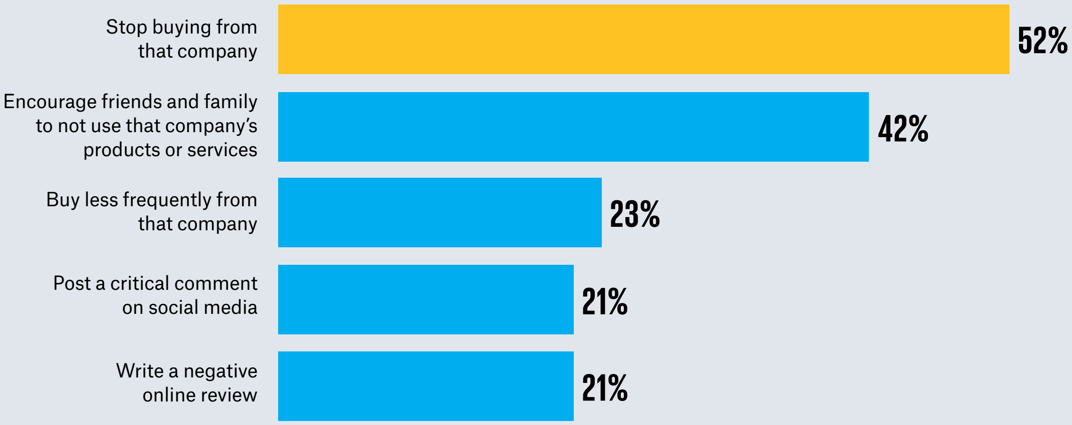


As incidents of computer hacking grow more frequent, consumers' trust in companies is declining. According to the Breach Level Index by business security company Gemalto, the number of hacking events rose globally 9 percent from 2014 to 2015

BOTTOM-LINE IMPACT

READY TO BOYCOTT A BUSINESS

What would you do in response to a breach?



Percentages do not total 100, due to multiple response options

In a clear indication of the reputational and financial risk from a data breach, more than half (52 percent) of consumers globally said they would stop buying from a company in the event of a breach. Nearly half (42 percent) said they would encourage others to join them. Consumers in France (60 percent), Brazil (58 percent) and Singapore (56 percent) appear the most likely to boycott a company

PREVENTION

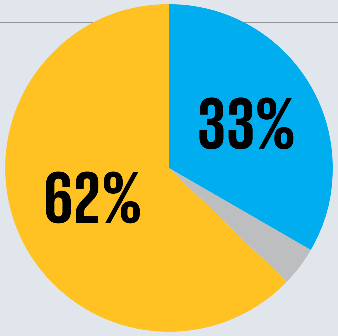
EXPECTATION OF MORE PROTECTION

Are companies doing enough to prevent data breaches?

🟨 Companies **are not doing enough** to prevent data breaches and need to take significant actions to improve the security of their storage systems

🟦 Companies **are doing enough** to prevent data breaches, but the rise in usage of debit cards, credit cards and online payment systems, as well as increased capabilities of online thieves, means that data breaches are just the "new normal"

⬜ Unsure

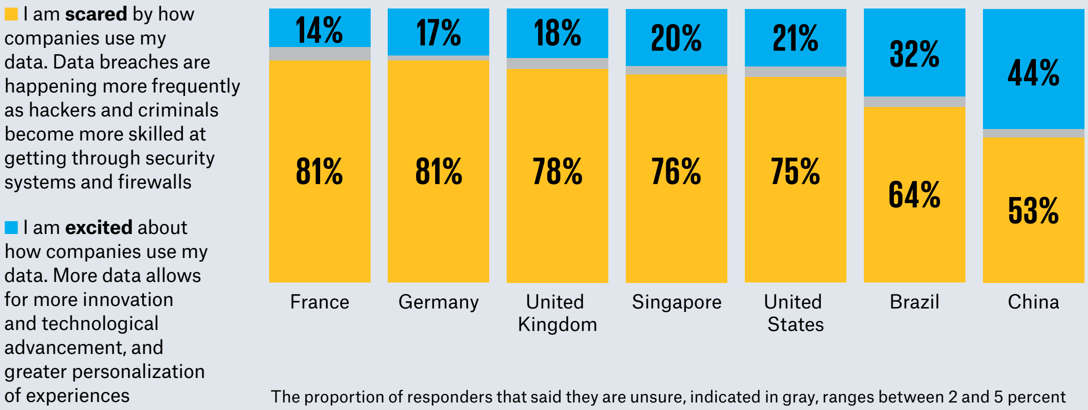


Aware that advances in digital technology are fueling the rise in breaches, consumers still feel companies should do more to improve the security of their personal information. Each of the first four months of 2016 saw an increase in records lost or stolen in data breaches, according to Gemalto

FEAR FACTOR

COMPANIES NEED TO COMMUNICATE BENEFITS

How do you feel about how companies are using personal data?



The proportion of responders that said they are unsure, indicated in gray, ranges between 2 and 5 percent

Communicating the positive role of data in a company's business can promote customer loyalty. However, getting past consumers' strong emotions around the security of their data can be a challenge. Survey responses use words such as "intrusive," "private" and "caution" to describe data collection practices. Turning that perception around requires a dedicated effort and clear messages

The heart rules the head

Good decisions need good feelings, says Brunswick's ROB ALEXANDER

We like to see ourselves as rational, sensible beings who make considered, data-led decisions, and when we describe a decision as emotional it is usually a synonym for poor or foolish. But how often have you decided to have "just one more glass," a muffin rather than an apple or taken the elevator rather than stairs? Our decision making is less rational than we like to think and often moves us to choose a less sensible path, or even one that may not be good for us.

This kind of behavior has a direct bearing on discussions about cybersecurity. People are the critical component of any company's data protection plan. How they feel about the company and its data policy colors how they behave.

Neurologist Antonio Damasio, in his 1994 book *Descartes' Error*, shows that people actually need emotions in order to make choices. The book features a case where the part of the brain that enables emotions was damaged; the patient had strong cognitive function and IQ scores but was almost totally unable to make decisions.

Yet it is obvious that emotions can lead to bad decisions. The code breakers at Bletchley Park during World War II cracked the highly complex Lorenz cipher as a result of a rash decision by an irritated German teleprinter operator. When a recipient requested a long, 4,000-character message be re-sent, the annoyed sender took shortcuts, using the same settings and, even worse, abbreviations to make his task easier. That breach of protocol was enough to allow the code to be broken. Armed with this key, the allies were eventually able to read Hitler's personal messages to his high command. (See "Colossus," Page 9.)

> **"Our decision making is less rational than we like to think and often moves us to choose a less sensible path"**

Emotions have also been shown to affect how we respond to the advice and input of others. In a study published by researchers at Harvard and Wharton in 2008, the accuracy of answers given by subjects varied dramatically according to their emotional state. Angry emotions led to accuracy being reduced by more than 30 percent and made subjects more inclined to disregard advice.

With a topic as sensitive as the use of personal data, or as detailed as a company data security policy, it is critical for a company to take into account this non-reasoning aspect of decision making. The best way to ensure a constructive response is to provide a positive emotional context.

ROB ALEXANDER is a Partner in Brunswick's London office. After 20 years as a strategic planner in advertising, he leads the Campaign Planning team.