Consumer Intelligence Series: Protect.me

An in-depth look at what consumers want, what worries them, and how companies can earn their trust—and their business.

Contents

How consumers see cybersecurity and privacy risks and what to do about it

How concerned are consumers about cybersecurity and privacy risks? Do they believe companies and the government are doing enough to protect their personal information? Do they feel they are in control of their data? And what does it take to win their trust?

We conducted extensive research to better understand consumer attitudes about data security, cybersecurity, privacy, trust, and regulation.

It's critical that companies understand and respond appropriately to their customers' cybersecurity concerns. To earn consumers' trust, you must vigorously protect customers' data while respecting individual privacy as you look for ways to monetize that data.

Methodology: *During August and September 2017, PwC surveyed a nationally representative sample of 2,000 Americans over the age of 18 via an online survey and video interviews.*

Key Findings:

69% of consumers believe companies are vulnerable to hacks and cyberattacks.

10% of consumers feel they have complete control over their personal information.

25% of consumers believe most companies handle their sensitive personal data responsibly.

72% of consumers believe businesses, not government, are best equipped to protect them.

For consumers, cyberattacks are personal

45% of respondents believe their email or social media accounts will get hacked in the next year—more than those who assume they'll have a flight canceled (36%) or get in a car accident (20%).

My email or social media accounts get hacked	45%
My flight is cancelled	36%
I get a new job	35%
I have to go to the ER	31%
I'm a victim of credit card fraud	29%
I win money in the lottery	25%
I get food poisoning	24%
My employer gets hacked/is subject to a cyberattack	21%
I'm involved in a car accident	20%
My identity gets stolen	18%
My insurance company refuses to pay a claim	17%
My home gets burglarized	8%

Q: Which is most likely to happen within the next year?
Source: PwC US Protect.me Survey, 2017

The stark reality is consumers trust companies less today than in the past. Only 12% of consumers said they trust companies more than they did a year ago, while 17% trust companies more today than a decade ago.

Consumer trust is fading

Can businesses be trusted to secure their customers' personal information? Consumers don't think so.

Just 25% of respondents believe most companies handle their sensitive personal data responsibly. Even fewer—only 15%—think companies will use that data to improve their lives.

If your customers don't trust you to protect their sensitive data and use it responsibly you'll get nowhere in your efforts to harness the value of that data to offer customers a better experience.

88% of consumers agree the extent of their willingness to share personal information is predicated on how much they trust a given company.

Nearly the same number (87%) of consumers say they will take their business elsewhere if they don't trust a company is handling their data responsibly.

Who's on the hook? Consumers say businesses more than government

92%
agree companies must be proactive about data protection

82%
say government should regulate companies' use of data

80%
agree government regulation of new technologies is crucial for consumer protection

72%
believe companies are better equipped than government to protect their data

70%
say government |is ineffective in ensuring fair use of their data

60%
say the responsibility of protecting data rests with the company collecting the data

Q: Which of the following industries or company types are the most trustworthy? Chose top five.
Source: PwC US Protect.me Survey, 2017

Who should be responsible for ensuring data is safeguarded and used responsibly?

Consumers want both companies and the government involved, but say companies bear a larger share of the responsibility.

Companies should do more than what's required by law—proactively managing cybersecurity and privacy risks in a way that goes beyond a compliance "checklist" approach.

Consumers also expect more from regulators when it comes to protecting data.

Unlike the European Union's approach to data privacy regulation—known as the General Data Protection Regulation (GDPR)—most US data privacy laws vary by sector, data type, or from state to state.

The path to trust: Giving customers control and providing transparency

Consumers want both companies and the government involved, but say companies bear a larger share of the responsibility.

Companies should do more than what's required by law—proactively managing cybersecurity and privacy risks in a way that goes beyond a compliance "checklist" approach.

Consumers also expect more from regulators when it comes to protecting data.

Unlike the European Union's approach to data privacy regulation—known as the General Data Protection Regulation (GDPR)—most US data privacy laws vary by sector, data type, or from state to state.

85%
of consumers **will not do business with a company** if they have concerns about its security practices

92% Say they should be able to control the information available about them on the Internet

91% Say companies should notify consumers about all data breaches

88% Say the amount of data they share with a company depends on how much they trust it

87% Want the ability to remove their personal data from the Internet if it hurts their reputation

85% Say cybersecurity and privacy risks are among the biggest risks facing society

71% Find companies' privacy rules difficult to understand

Q: How much do you agree or disagree with the following statements?
Source: PwC US Protect.me Survey, 2017

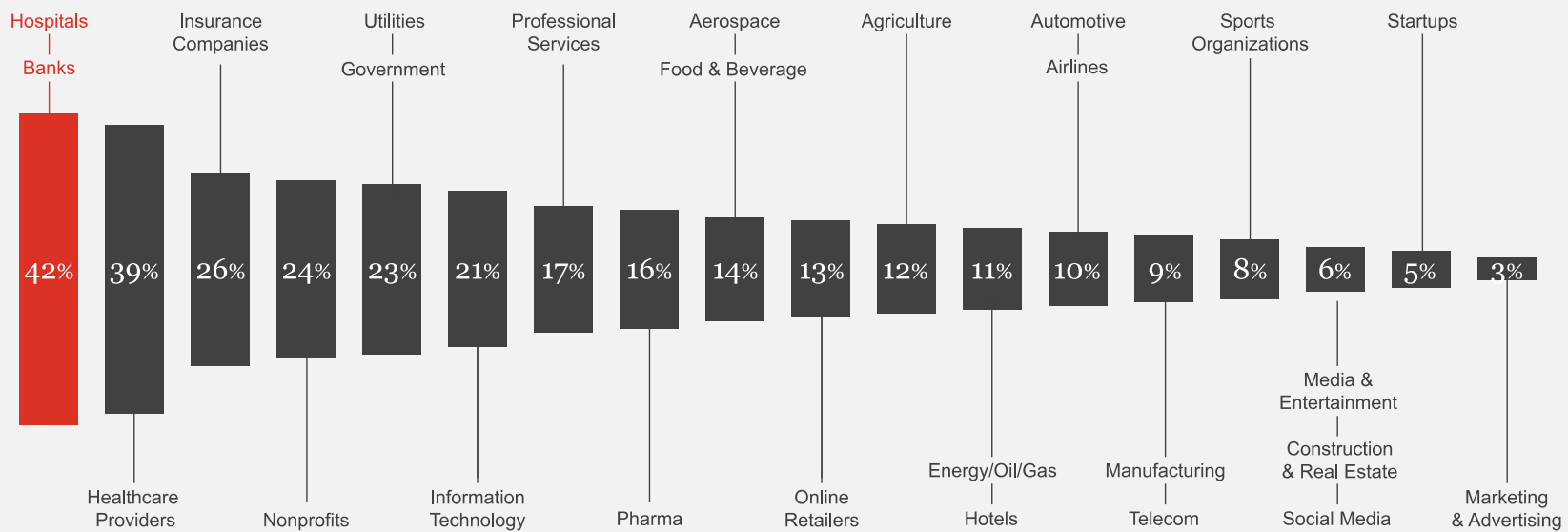# Consumers want control over their data, but don't feel like they have it

Only 10% of consumers feel they have complete control over their personal information.

More than half of consumers (53%) say they'd make an effort to get their personal information back from a company if they had the option.

The stakes are high. If companies don't adequately protect consumer data, they risk suffering consequences from regulators and backlash from consumers who say they will take their business elsewhere.

71% would stop doing business with a company for giving away their sensitive data without permission.

# What types of businesses do consumers trust most?

Hospitals | Banks — 42%
Healthcare Providers — 39%
Insurance Companies — 26%
Nonprofits — 24%
Utilities | Government — 23%
Information Technology — 21%
Professional Services — 17%
Pharma — 16%
Aerospace | Food & Beverage — 14%
Online Retailers — 13%
Agriculture — 12%
Energy/Oil/Gas | Hotels — 11%
Automotive | Airlines — 10%
Manufacturing | Telecom — 9%
Sports Organizations — 8%
Media & Entertainment | Construction & Real Estate | Social Media — 6%
Startups — 5%
Marketing & Advertising — 3%

Q: Which of the following industries or company types are the most trustworthy? Chose top five.
Source: PwC US Protect.me Survey, 2017
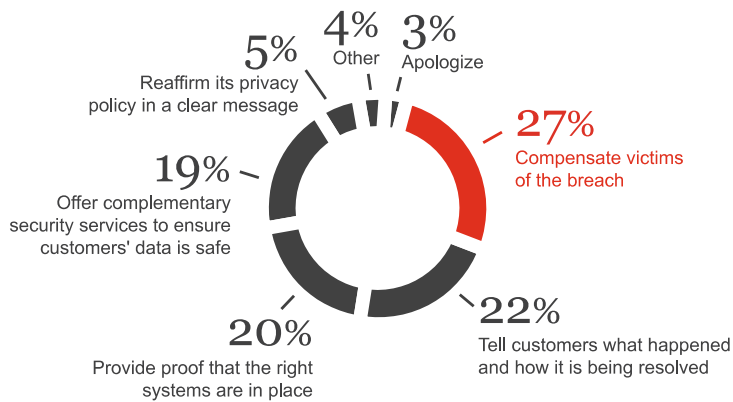
Consumers' trust varies by industry

In PwC's 20th Global CEO Survey, 69% of CEOs said it is becoming much more difficult for businesses to earn and keep trust in a digital world.

Our research on consumer attitudes found that their trust varies by industry.

- Banks and hospitals tie as most trusted when it comes to privacy and cybersecurity, outranking healthcare providers, nonprofits, and online retailers.

- Social media companies, advertising agencies and startups are less trusted than firms in other sectors and need to be proactive in maintaining consumer trust.
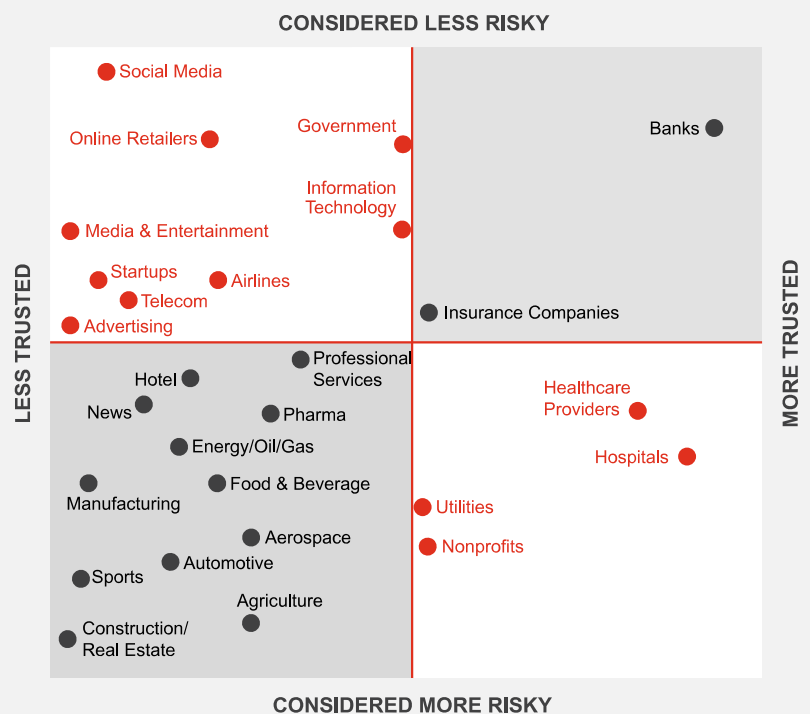
Q: Which of the following industries or company types are the most trustworthy?
Source: PwC US Protect.me Survey, 2017

5% Reaffirm its privacy policy in a clear message

4% Other

3% Apologize

27% Compensate victims of the breach

19% Offer complementary security services to ensure customers' data is safe

20% Provide proof that the right systems are in place

22% Tell customers what happened and how it is being resolved

Q: What's the best way for companies to regain your trust after a hack or other data breach?
Source: PwC US Protect.me Survey, 2017

After a data breach, can companies earn back consumer trust?

Consumers are willing to forgive, but their trust can only be regained if companies implement real changes in the wake of a breach.

Although no one action will win back every customer, some measures are more likely to resonate with consumers—including compensation for victims, a detailed explanation of what happened, and a clear description of the privacy policies in place.

Consumers want businesses to be responsive, transparent, and take steps to ensure a breach does not happen again.
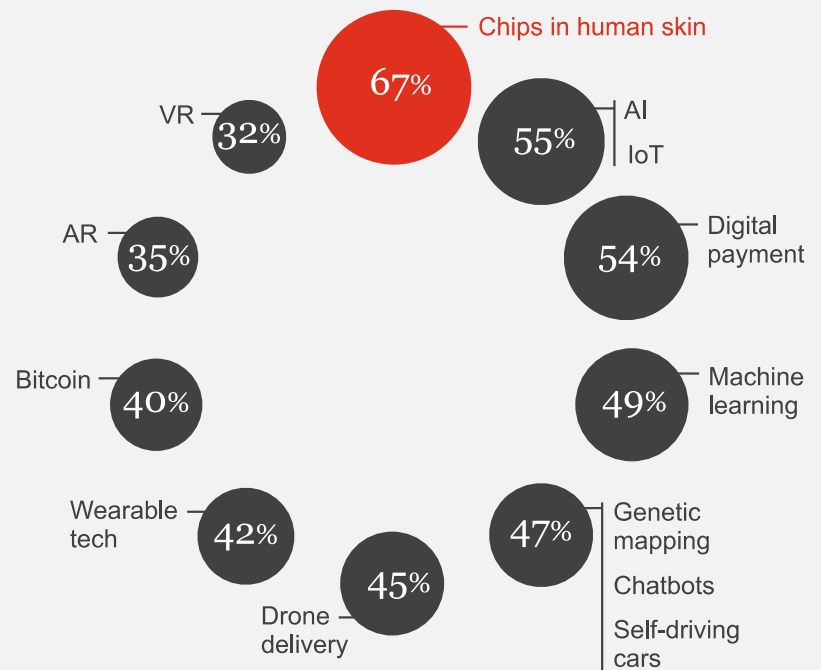
Consumers see some emerging technologies as a risk to their privacy

Consumers are concerned about the cybersecurity and privacy implications of certain emerging technologies.

25% of consumers see our growing reliance on technology as one of the top threats facing humanity over the next 50 years.

In response, businesses are starting to focus on strategies and investments to counter such risks, although according to our Global State of Information Security® Survey, most companies have yet to implement an integrated Internet of Things (IoT) cybersecurity program.

As emerging technologies such as artificial intelligence and the IoT take root, governments and businesses may be forced to explore comprehensive new measures to address consumers' data and privacy rights.

Chips in human skin 67%

VR 32%

AR 35%

Bitcoin 40%

Wearable tech 42%

Drone delivery 45%

AI 55%
IoT

Digital payment 54%

Machine learning 49%

Genetic mapping 47%
Chatbots
Self-driving cars

Q: How big of a threat to privacy and security is each of the following technologies?
Source: *PwC US Protect.me Survey, 2017*

A call to action driven by customers' concerns

As the frequency and scale of data breaches continue to rise, so do consumer worries. Companies must understand and address these concerns or risk losing business. To thrive in the new data economy, companies should:

Prioritize cybersecurity and privacy - Putting cybersecurity and customers' privacy at the forefront of your business strategy—and backing it with proven security tactics—can help address consumer concerns and cement their loyalty.

Build trust through action - Rhetoric alone is not enough. Companies must implement robust data governance and give consumers more control over how their personal information is used.

Go beyond existing regulations - Consumers don't think regulation is keeping up with innovation. Companies that do more than what's required by law are likely to earn consumers' trust.

Understand how consumers feel - Companies in industries considered less trustworthy should be particularly proactive in addressing consumers' concerns.

Be transparent when using new technology - Companies that demonstrate they are using emerging technologies responsibly and transparently—and for consumers' benefit—will not only strengthen customers' trust, but also make it easier to engage with customers on a deeper level.

The bottom line

Companies must put cybersecurity and privacy at the forefront of business strategy to win customers' hearts—and earn their trust. And they must implement, meet, and clearly communicate robust data governance and privacy protection policies.

Request a meeting with our specialists

David Sapin
Principal, Risk and Regulatory
Tel: +1 (202) 756 1737
david.sapin@pwc.com
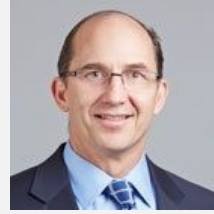
Sean Joyce
US Cybersecurity and Privacy Leader
Tel: +1 (703) 918 3528
sean.joyce@pwc.com

Jocelyn Aqua
Principal, Cybersecurity and Privacy
Tel: +1 (202) 730 4862
jocelyn.aqua@pwc.com

Jay Cline
US Privacy Leader
Tel: +1 (612) 596 6403
jay.cline@pwc.com

Matthew Lieberman
Advisory Marketing Leader
Tel: +1 (213) 217 3326
matthew.lieberman@pwc.com

pwc.com/CIScyber