KPMG

Consumer Loss Barometer

kpmg.com

Consumer Loss Barometer:

Business value hinges upon cybersecurity

Cybersecurity: At the surface, this is an "all hands" IT issue

Go beneath, and it is something even deeper than that.

Amid the proliferation of data, more and more companies are gathering vast quantities of information and gleaning insights about their customers to improve business growth, products, services, and the overall customer experience.

As they do so, at what point does cybersecurity become less of an IT challenge, and more of a core component of the fundamental business?

Closely related are customers' current attitudes toward cybersecurity. How do customers feel about data security? What do they expect in the event of any "incident"? What must a company do to minimise the pain of any financial identity or similar data privacy misstep?

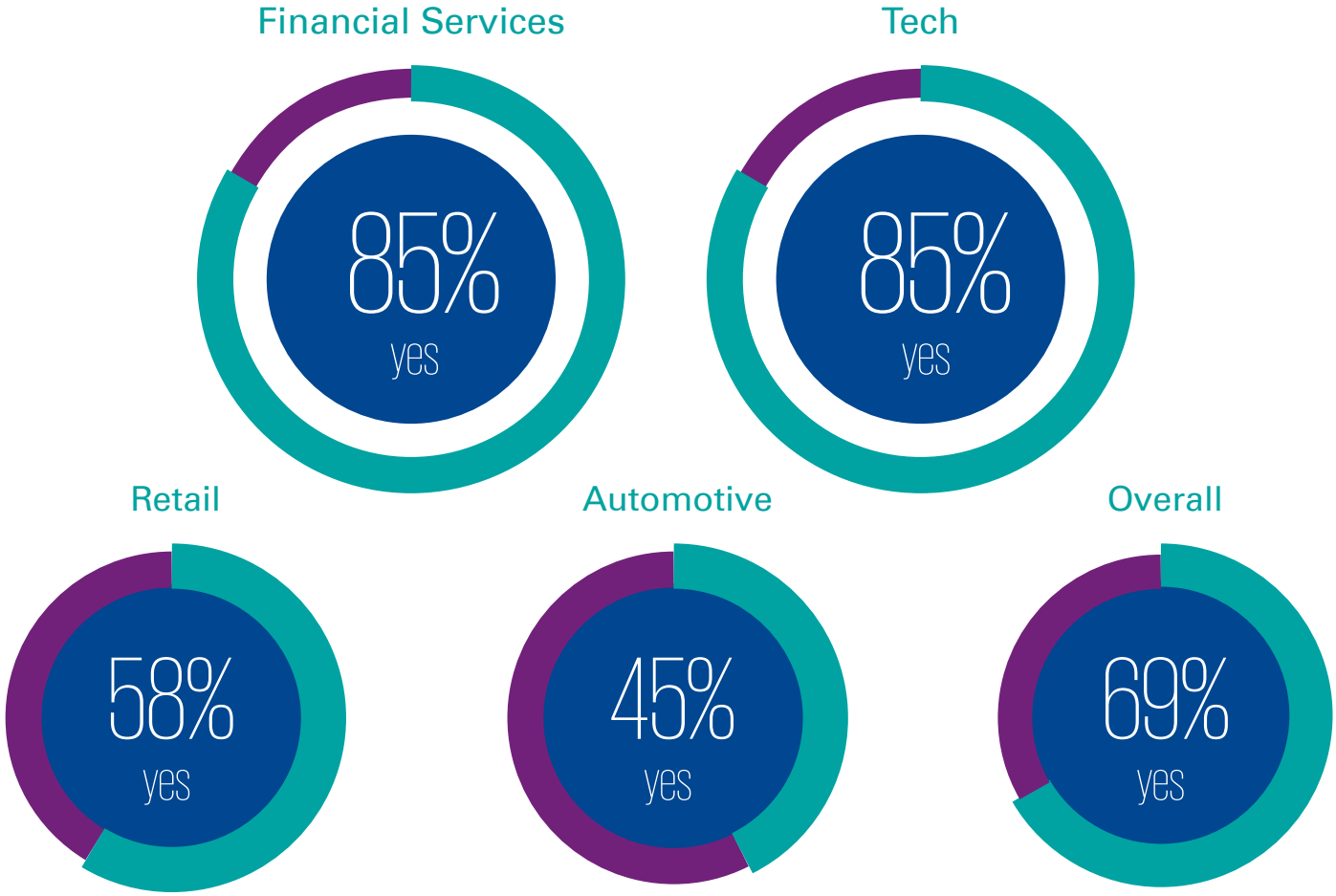
Forbes Insights and KPMG surveys of 403 corporate executives and 750 consumers provide deeper understanding of how cybersecurity management — or mismanagement — can create or destroy value.

"In too many industries, information security is still seen as a technology risk to be minimised instead of a business issue to be optimised."

– Greg Bell
U.S. Leader,
KPMG Cyber

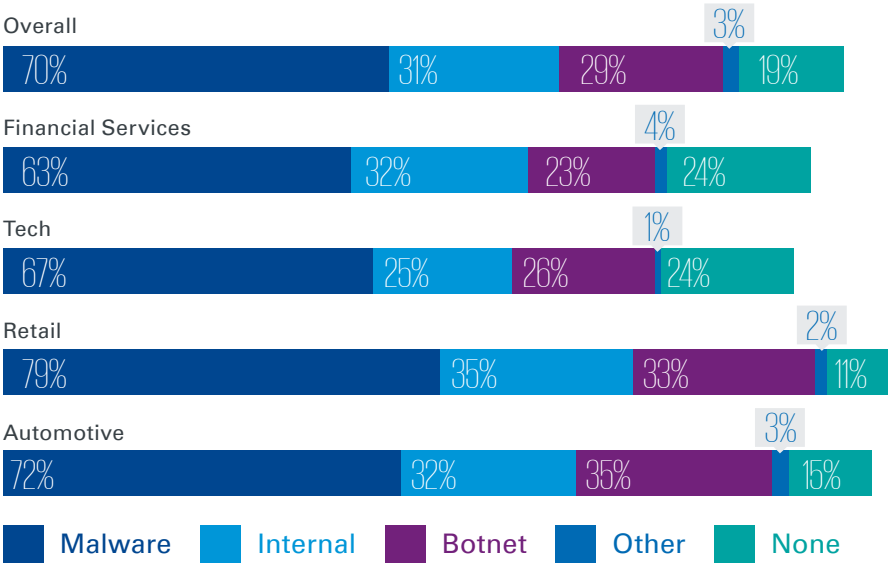
The business view: Assessing threats and opportunities

Is there a leader whose sole role is information security?
Retail and automotive are relative laggards.



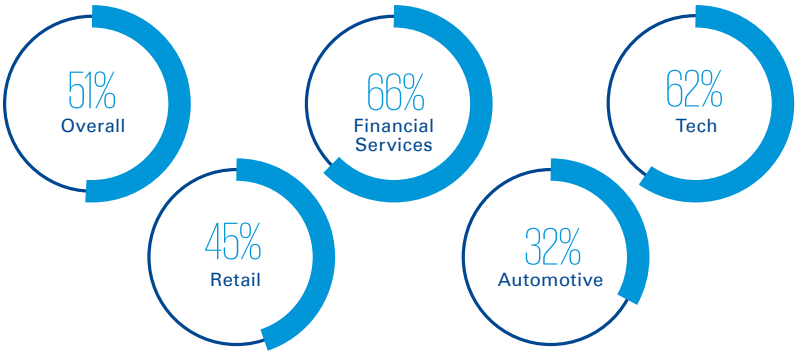
In the past 12–24 months, what attack vectors have your organisation experienced?

Attacks are rampant — across a variety of vectors.



Has your firm used capital funds to invest in information security in the past year?

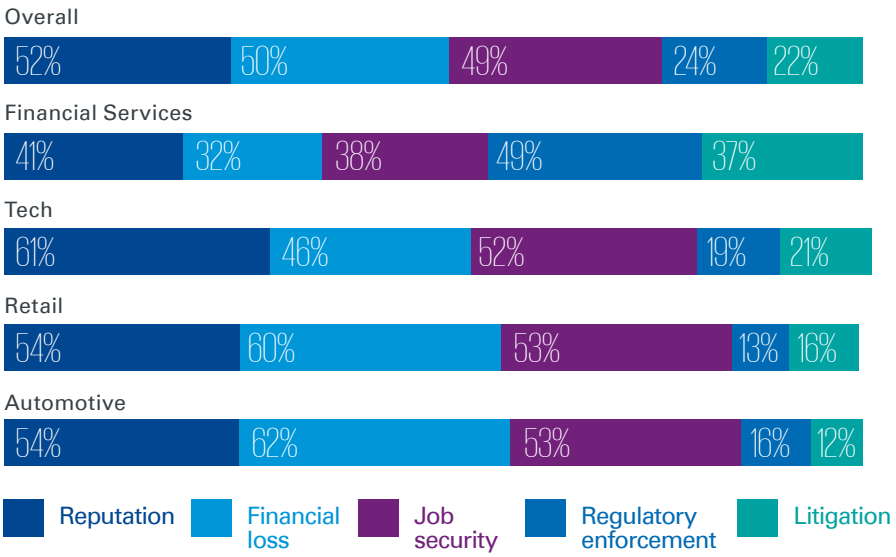
Retail and automotive are again lagging.



Note that legacy automakers are relative newcomers to the risks of cybersecurity — and may be underfunding related initiatives.

What are your top concerns in a breach?

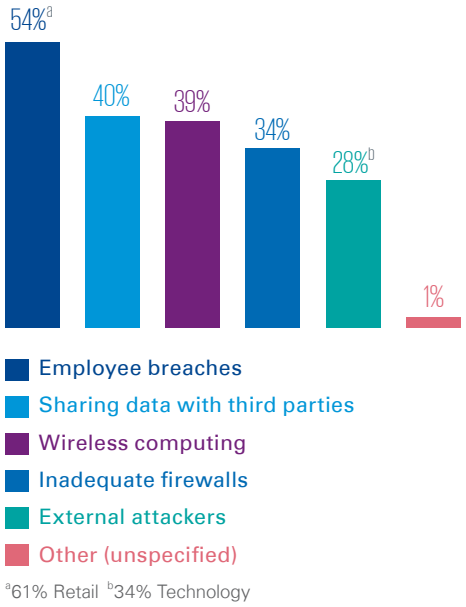
The risks are many and costly to both the organisation's stature and bottom line.



[x] Regulatory enforcement can shut down a bank, often leading banks to focus primarily on known threats — already regulated — instead of emerging threats.

In which of the following areas do you see the greatest vulnerabilities in your organisation's data security?

Employees are the weakest link in cybersecurity.



[a]61% Retail [b]34% Technology

> "Cyber risk teams within IT prefer a rigid operating model with little or no change other than updates to security processes. Business units, meanwhile, need growth — and that means agility, measured in days and weeks, not months and years. In an era where both agility and data security are essential, companies must achieve vastly greater alignment between their business units and IT."
>
> **— Greg Bell,**
> US Leader,
> KPMG Cyber

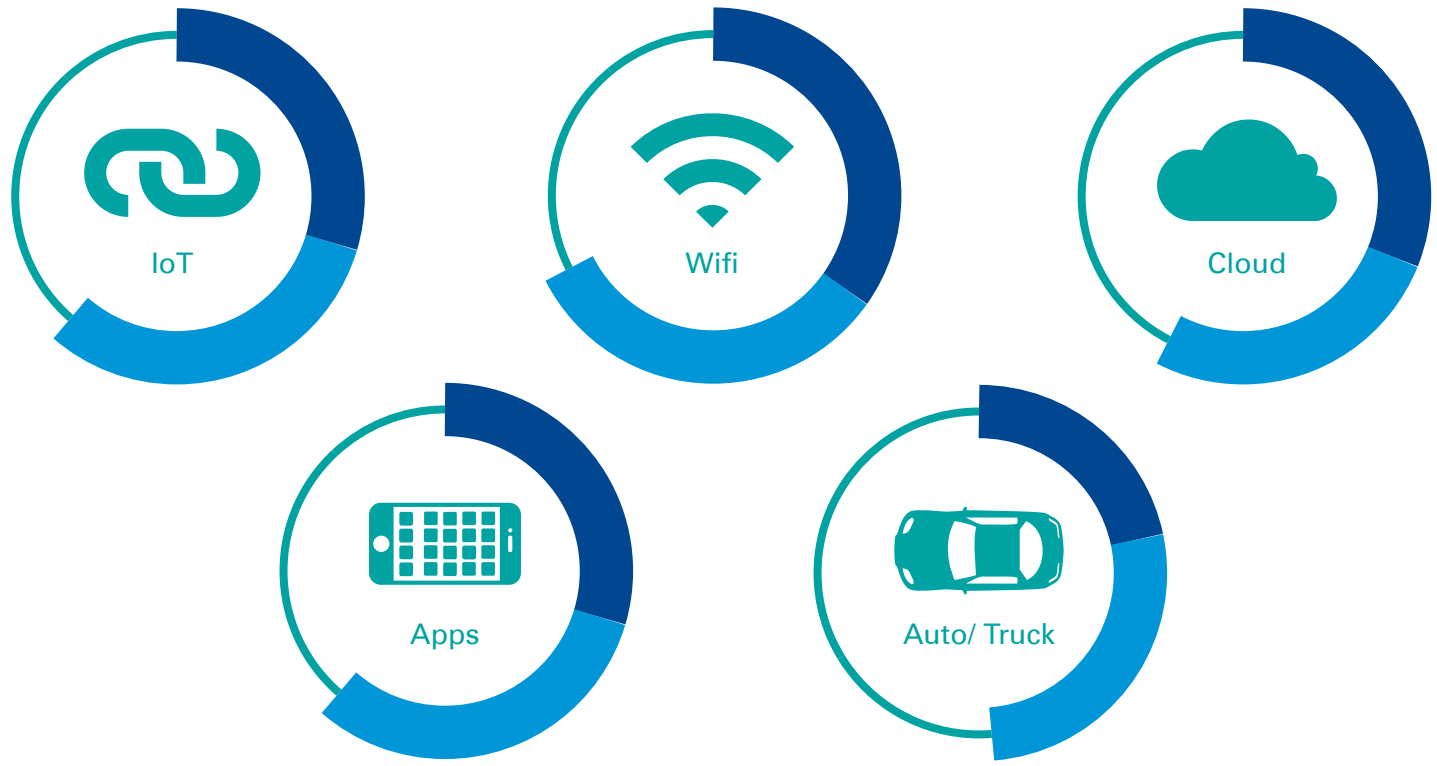
Sector by sector:

How consumers perceive cyber breaches

The consumer survey executed for this report looks at five specific product/service tracks asking: How concerned are consumers — and what steps should companies consider to mitigate any damage caused by cyber breaches?

How concerned are you by the prospect of you, personally, experiencing any of the following products/services being hacked?[1]

Concern is evident across all consumer segments.



[1]Banking/financial services delivers similar results, but findings are excluded in this chart due to variance in the form of question posed.

Though concerned by the possibility of hacking, most consumers seem willing to forgive and forget, provided companies:

- Cover any losses promptly
- Communicate with transparency in the event of any breach
- Show that proactive steps are being taken to prevent future lapses in personal data and related security breaches.

These findings are relatively consistent across all sectors considered.

Banking / financial services:

If your personal accounts were hacked, what would lead you to close your accounts and move to a new institution?

Consumers expect their institutions to act quickly and to take responsibility.

Bank's refusal to cover losses

A lack of timely acknowledgement/response (providing details of the incident and impact on customers)

Lack of a solid plan to prevent future attacks

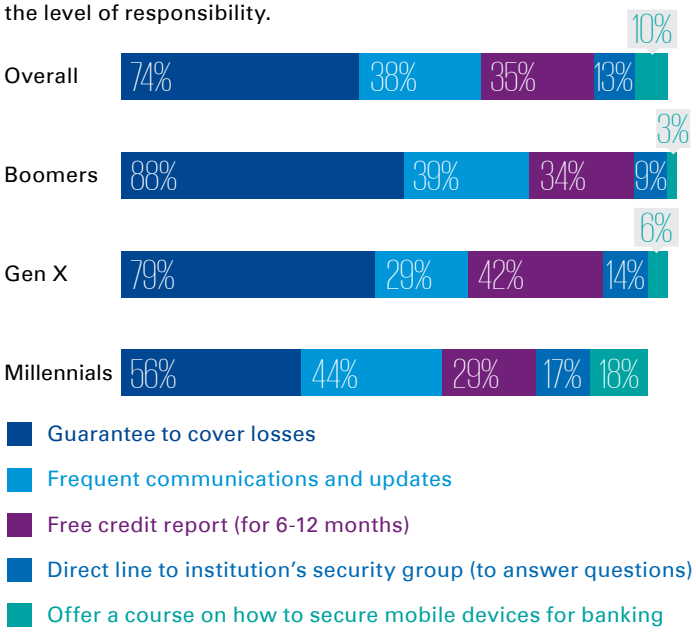
Learning about the incident via the press before being informed by the bank

All of the above[a]

[a]60% Boomers

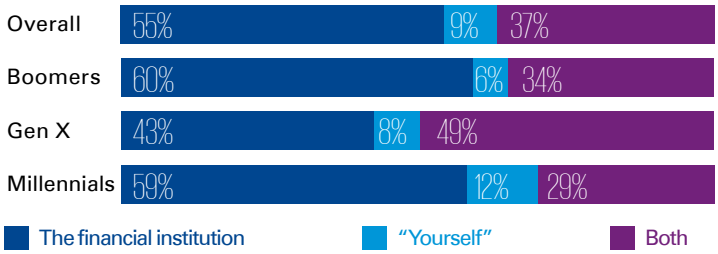
What action(s) do you expect your institution to take to help reduce concerns related to an information security breach/loss of your data?

Key differences between boomers and millennials regarding the level of responsibility.



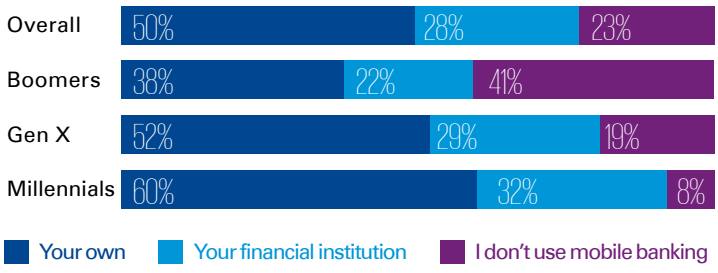
Who is to blame if you use mobile banking and your personal accounts are hacked?

Consumers say the institution bears most of the risk.



Whose responsibility is it to ensure mobile devices are secured for mobile banking?

Millennials feel they share the burden.



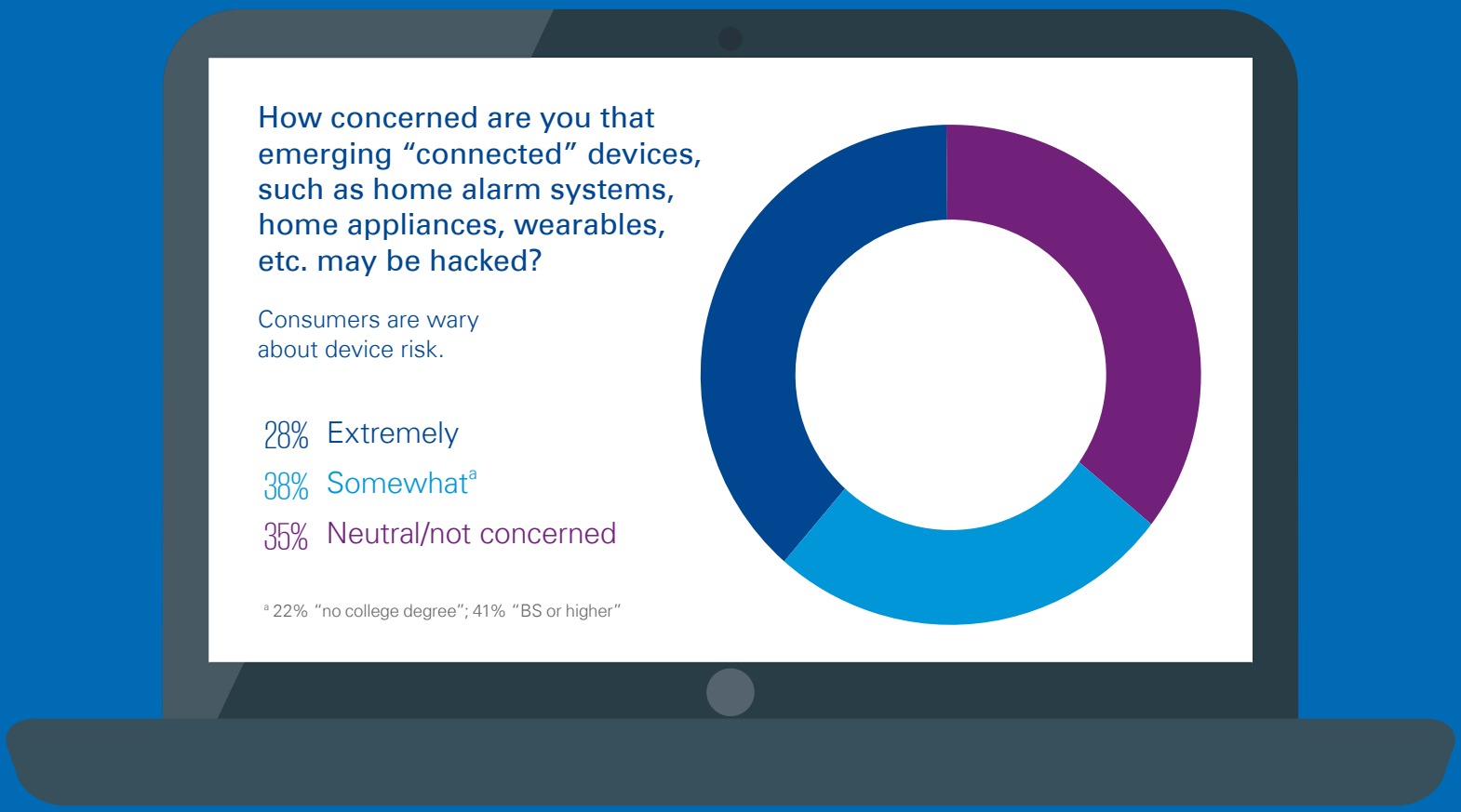
"Nearly three out of four consumers are using mobile banking — almost 90 percent of millennials. There is an opportunity for banks to better retain their customer base and solidify the trust that their customers have in their banking platform by showing that security is a top-line issue and they have a unique solution. In other words, for financial institutions who get it right, this is a brand-building and growth opportunity."

— Jitendra Sharma,
Advisory Line of Business Leader,
Financial Services

Connected devices / social media

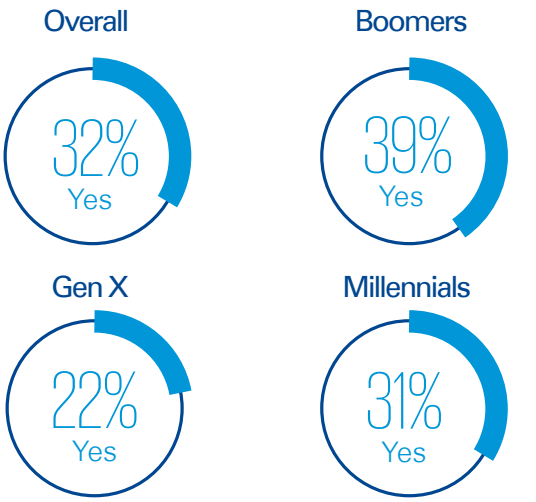
"Whether consciously authorised or not, by simply turning on a product or service, customers are today sharing vast caches of both device usage and personal data. Companies entrusted with this data need to recognise: cybersecurity and data protection is no longer an internal IT risk, but rather a strategic business risk of the highest order. Reputation, brands, trust and sales are all at risk. But with risk comes opportunity for those businesses who can pair cybersecurity with product and service development and delivery."

— Gary Matuszak,
Global Chair, Technology,
Media and Telecommunications,
KPMG LLP



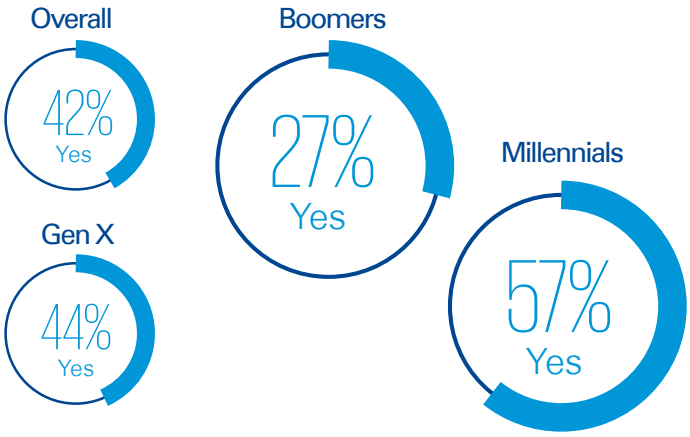
Have you limited your use of IoT devices due to security concerns?

Boomers are the most wary.



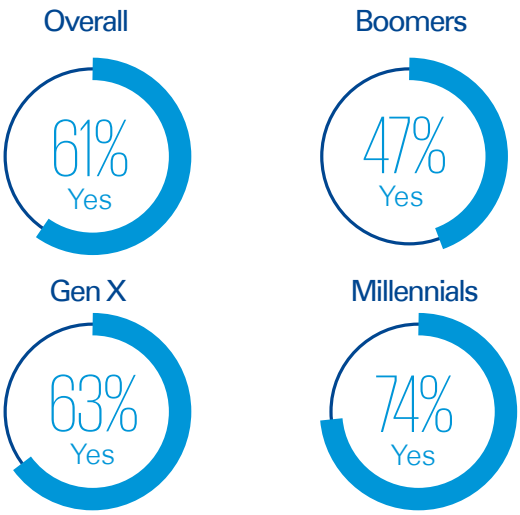
Would you store more personal information on your cloud/social media accounts or use them more if you had greater confidence in their security?

Millennials can be won over; Boomers not so much.



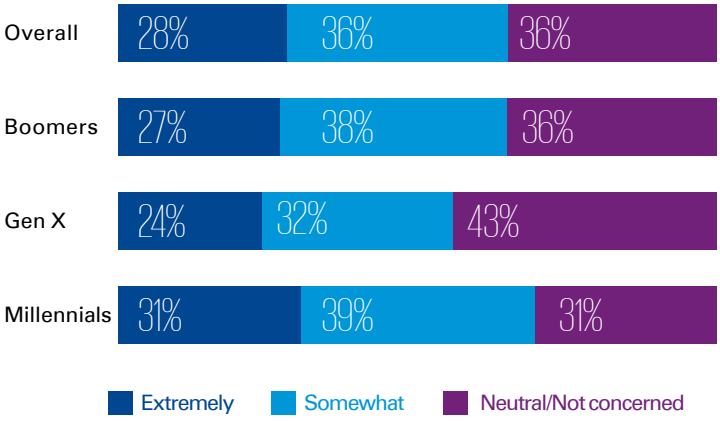
Would you use more IoT/connected devices if you had greater confidence in their security?

Consumers value a greater sense of security.



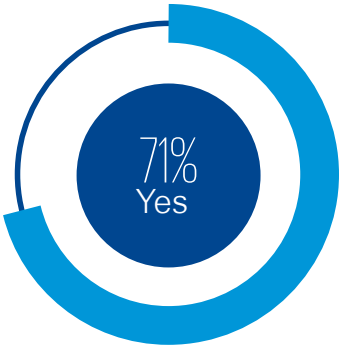
How concerned are you that your cloud or social media platform may be hacked?

Generations share concerns relatively equally.



If your cloud/social media account was hacked and your personal information as well as postings and photos were exposed/stolen, would you switch/disable cloud/social media providers because of this hack?

Where options exist, consumers will switch.[1]



[1]No significant differences by generation.

"There is a maturity curve with cloud/social media as it is nearly a decade old. With maturity and awareness, consumers can see the risks of putting too much information forward — so many are curbing what they share. But overall, companies need to evaluate the security/privacy balance from the customer's perspective: is the use of my device worth its risk? Security is today an inseparable component of any product or service."

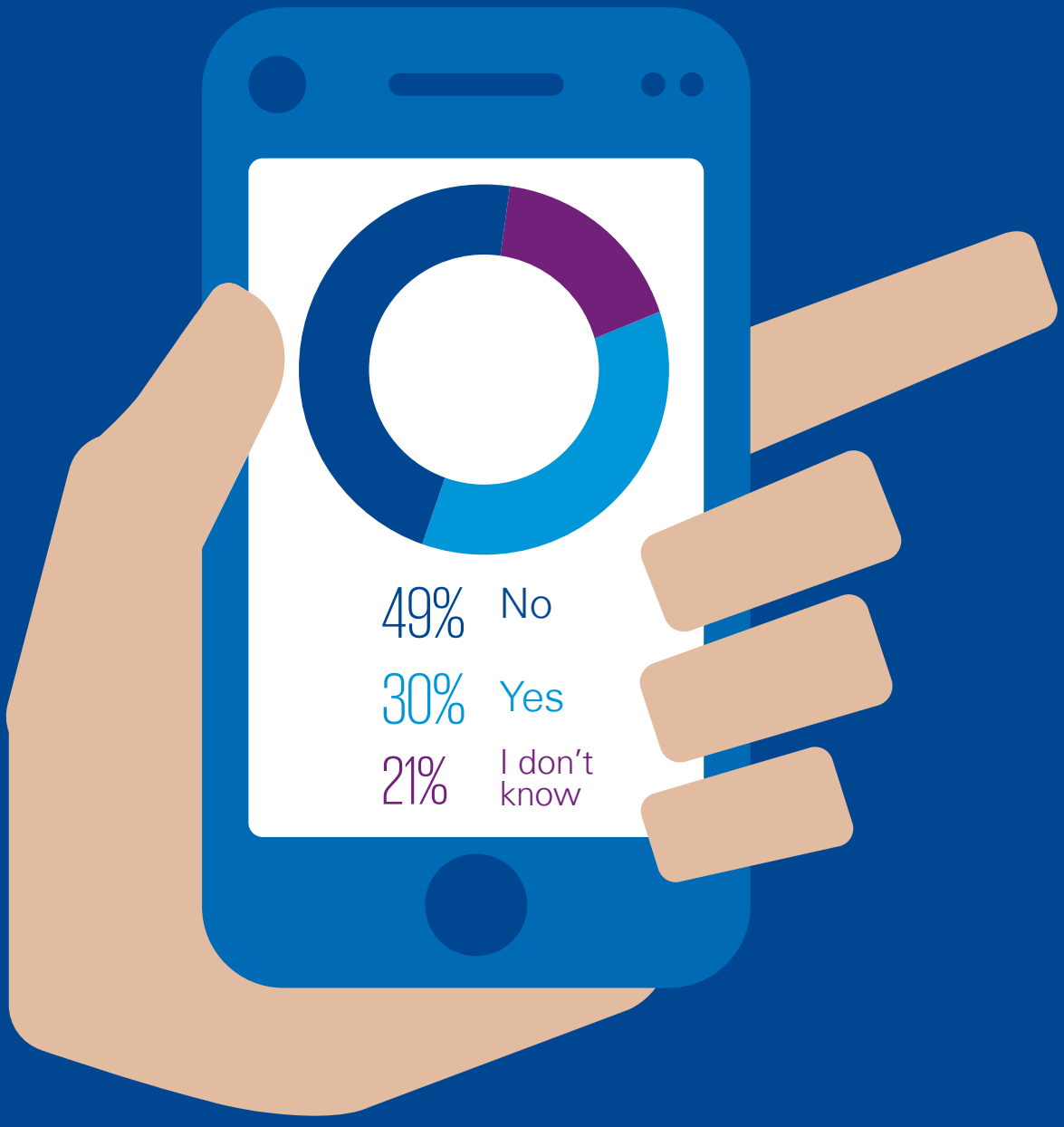
— Gary Matuszak,
Global Chair, Technology, Media and Telecommunications, KPMG LLP

Mobile

Wi-Fi, applications, mobile phone/devices

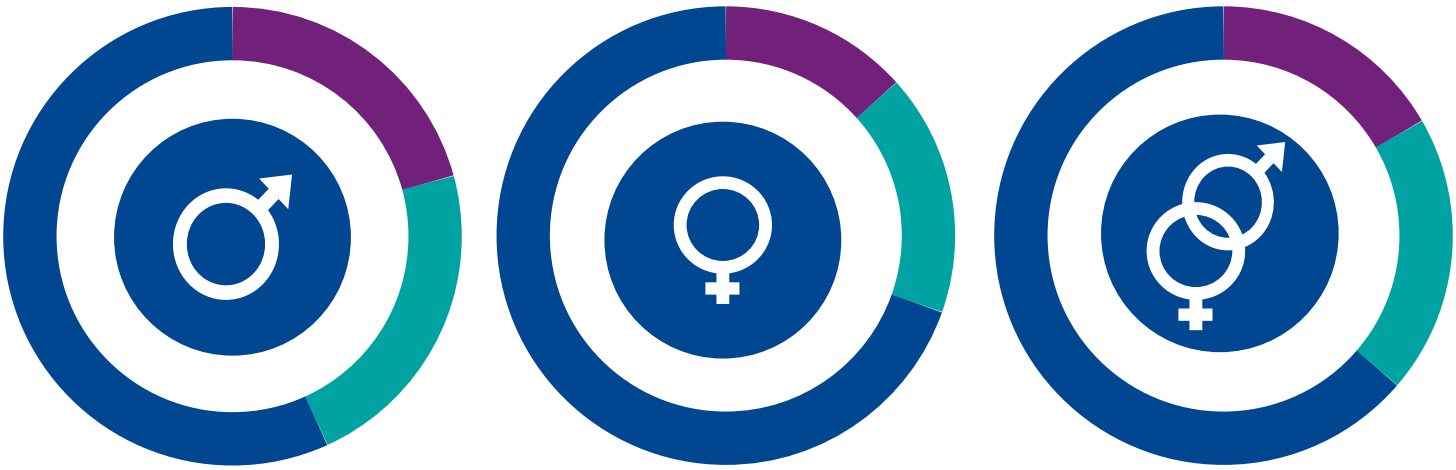
The mobile phone carrier that you use was recently the victim of a cybersecurity hack and the company took the steps to fix the problem and assure that people's personal information was secure. However, as a result of the hack, it became known that the carrier was covertly working with the US government to be able to hack into a person's mobile device and monitor information if the person is suspected of being involved in terroristic activities. If you believed that another carrier was not allowing this government access, would you be inclined to switch carriers to another carrier not allowing access?

A third or more of your customers may switch.



Your carrier discloses it has been tracking personal information that has now been hacked. A competing carrier responds by offering guarantees that no personal data will be collected. Do you switch carriers?

Security sells.

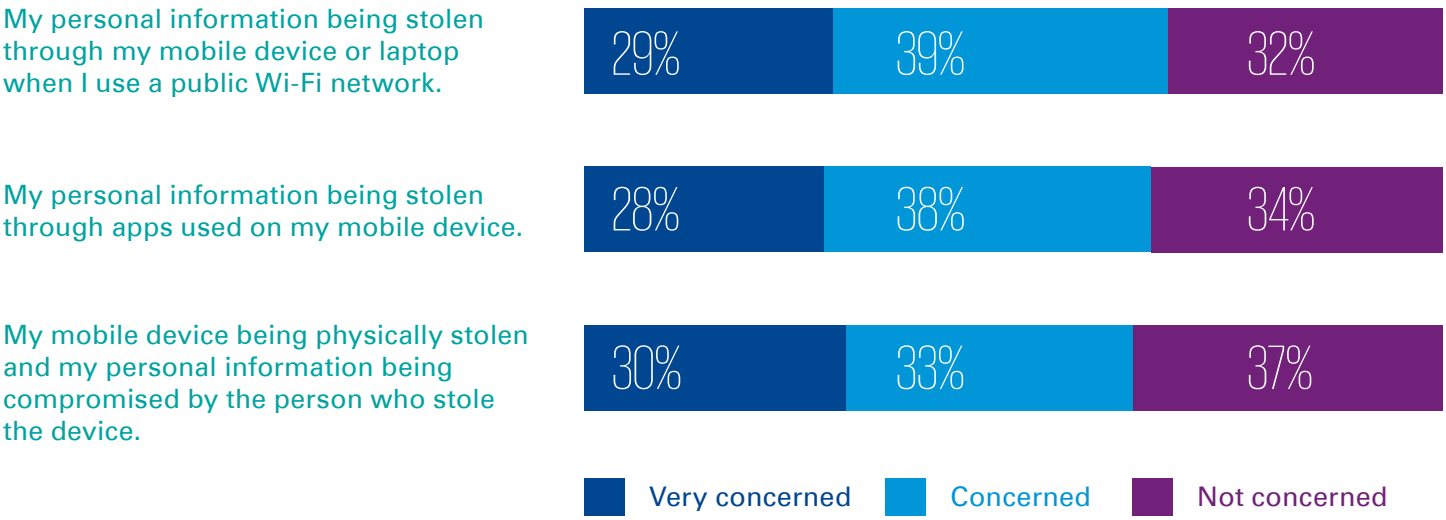


Yes, as long as the pricing remained competitive

Yes, even for a moderate premium

No

How concerned are you by:



"Overall, consumers aren't as confident as they could be in the security of their mobile devices and data. As Wi-Fi grows and next-gen mobile software and hardware comes to market, providers can differentiate themselves by educating consumers on device security and by then providing secure products and services."

— Paul Wissmann,
Partner, National Sector Leader,
Telecommunications and Mobile, KPMG LLP

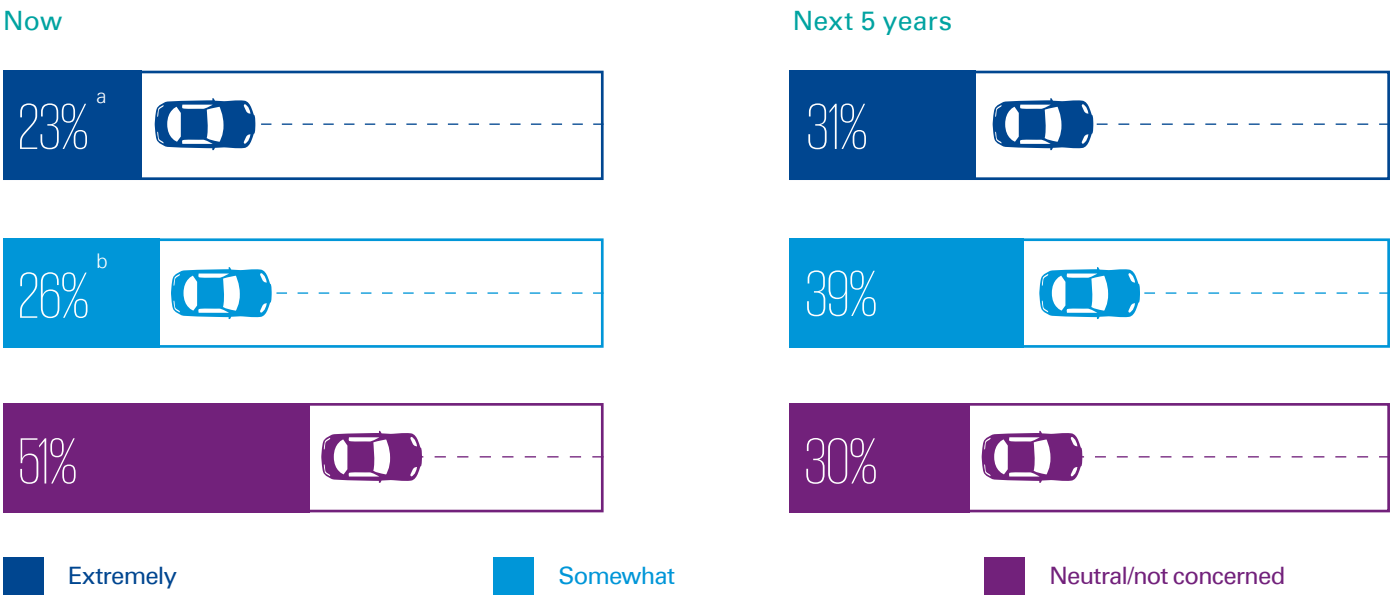
Connected automotive

"The statistics show that financial services customers are relatively forgiving in the event of a security breach: make amends and they will stay. Automotive customers are, by comparison, far more likely to abandon a brand over cybersecurity issues. This points to a maturity/ awareness curve: customers in banking are accustomed to hearing about security whereas in automotive, they may not even be aware the risk exists. Accordingly, the risks and costs of a misstep may be greater in auto than for many more 'tech-mature' industries."

— Gary Silberg,
Americas Head of Automotive, KPMG LLP

How concerned are you by the possibility that your car will be hacked?

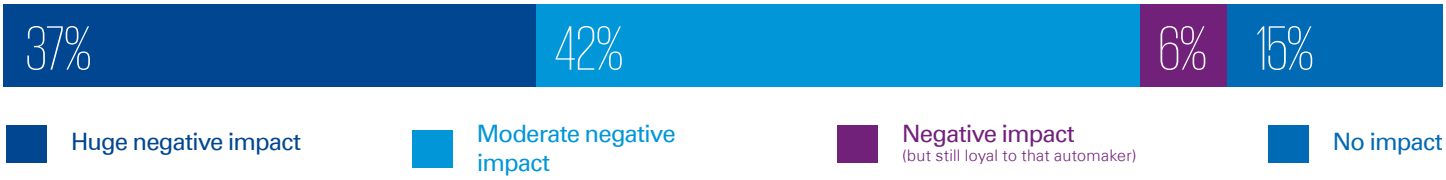
Awareness and concern are on the rise.



[a] 32% Millennials; 32% $100–$149,999
[b] No college degree 16%

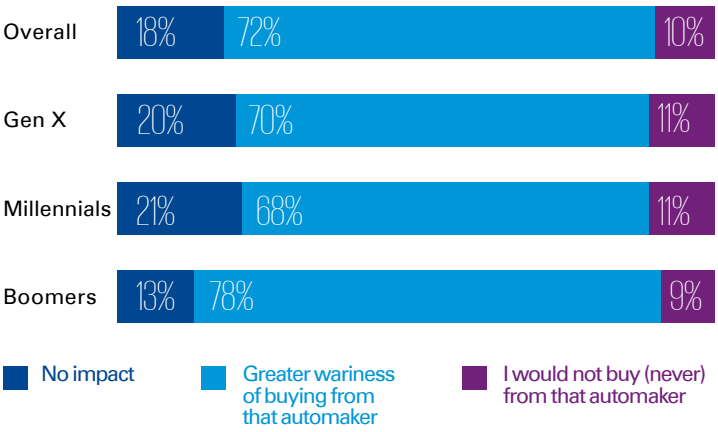
If your car was hacked, how would that change your perception of that particular automaker?

Your brand is at risk.



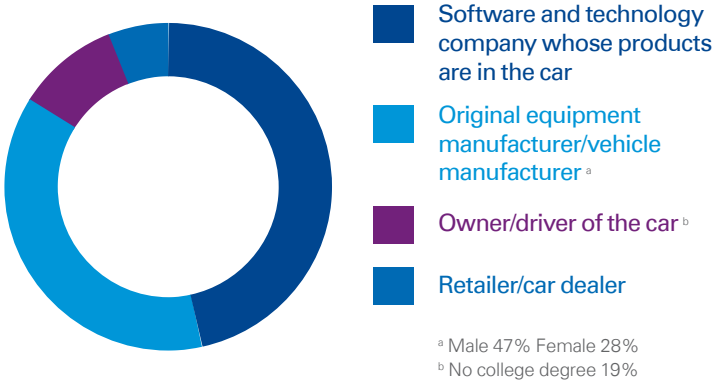
If a particular vehicle brand was hacked, how would that impact your consideration to purchase from that particular automaker?

Your sales are at risk.



Who should be responsible for the security of your connected car information?

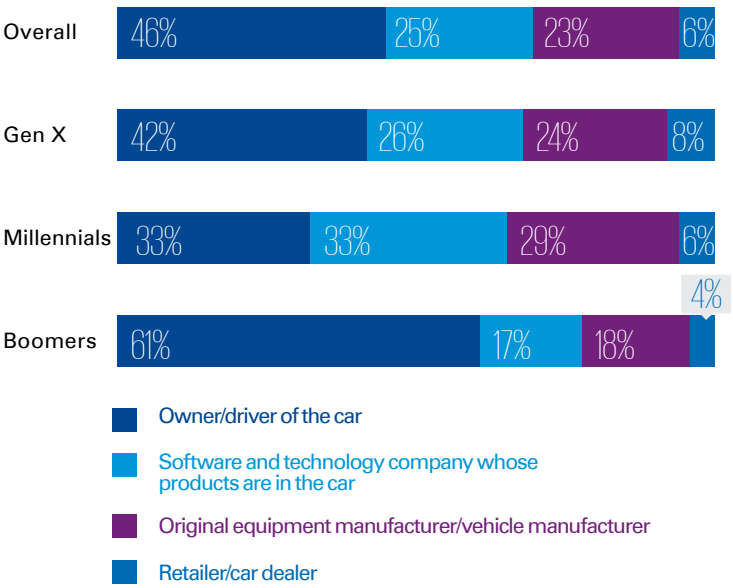
Owners believe liability is elsewhere.



[a] Male 47% Female 28%
[b] No college degree 19%

Who should be the guardian of your consumer and vehicle data?

A generational divide.



What scares you the most about your vehicle being hacked?

Safety is the chief concern.

41%[a] Someone else taking control of the vehicle

25% Personal financial information being stolen

15% My location being tracked without my knowledge

6% Personal photos/media content being stolen

2% Adherence to traffic laws

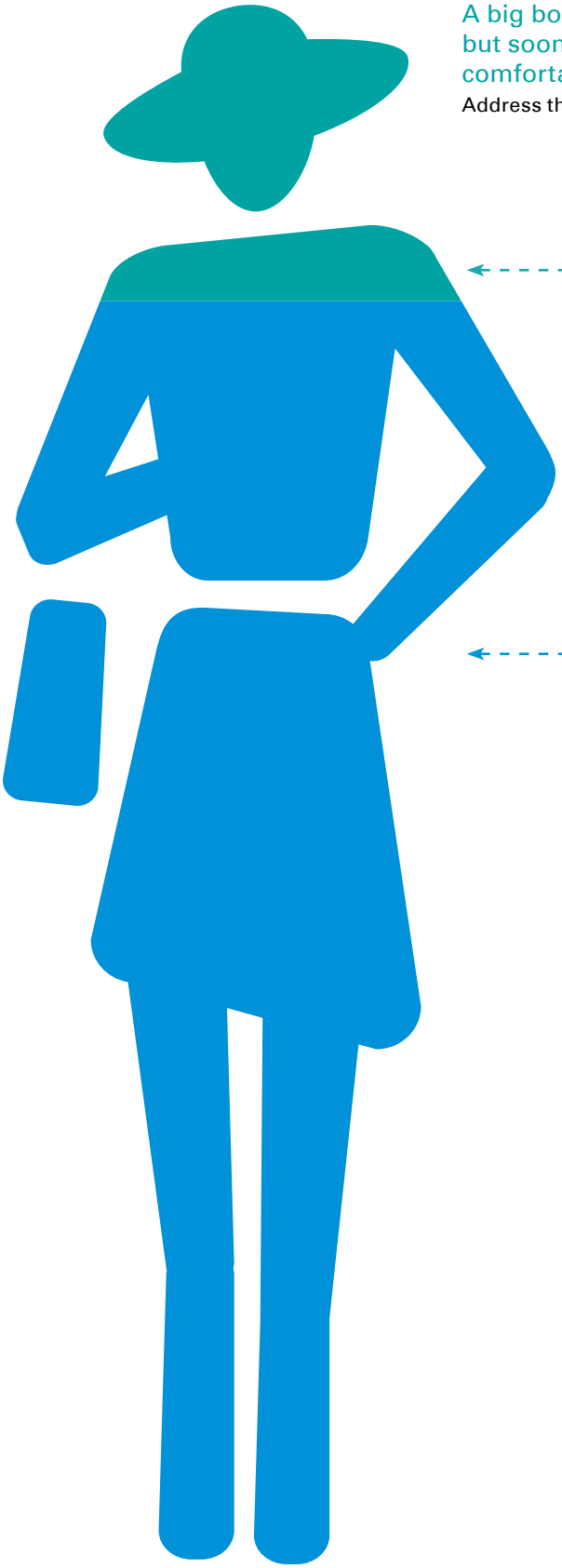
[a] 51% boomers

Note that one in ten, 11%, are not at all worried

"Cars and trucks today have evolved into highly complex computers on wheels, with many specialty companies providing the high-tech components and software. This increased connectivity presents some real and important cybersecurity risks, the most significant of which is safety. Unlike most consumer products, a vehicle breach can be life-threatening, especially if the vehicle is driving at highway speeds and a hacker gains control of the car. That is a very scary, but possible scenario, and it's easy to see why consumers are so sensitive about cybersecurity as it relates to their cars. In addition to safety, these new connected cars contain so much of our personal information — from apps and entertainment to location and personal financial information. Due to the potentially enormous damage to their brands and their sales, addressing cybersecurity concerns is a critical priority for automakers and one they cannot afford to get wrong."

— Gary Silberg,
Americas Head of Automotive,
KPMG LLP

Retail



A big box retailer is hacked, compromising your personal information, but soon thereafter addresses the security flaws. Would you still feel comfortable to continue shopping at that store?

Address the flaws; allay the fears.

19% No

81%[a] Yes

[a] 62% $25,000 to $34,000

If yes, how long would it take for you to feel comfortable buying from that retailer, online or in-store?

Losses can mount from slow-to-return customers.

48% Immediately
33% Three months
16% Six months
2% 12 months
1% More than 12 months

What factors would most likely contribute to you not shopping there again?

68%[a] Lack of a solid plan to prevent future attacks

54%[b] Retailer's refusal to cover losses

53%[c] Lack of timely acknowledgement/ response

51% Informed by the press before being informed by the retailer

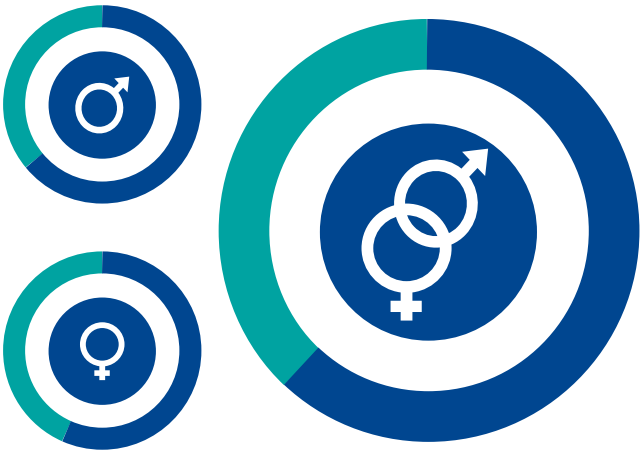
[a] 77% Boomers
[b] 71% Less than $25,000 ; 65% no college degree
[c] 63% Male; 44% Female

Cybersecurity: Mobile-pay apps

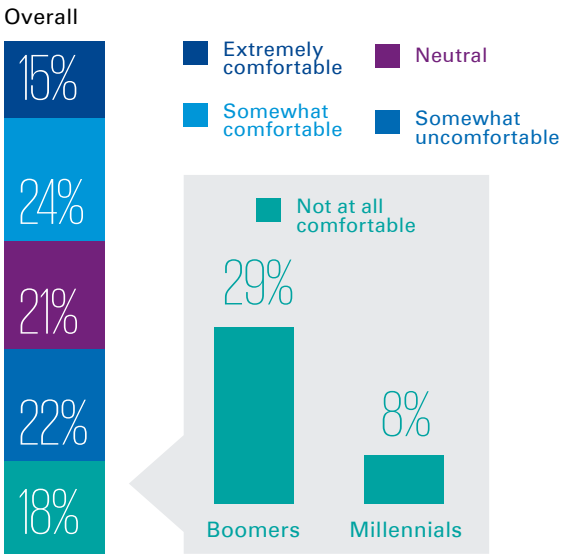
When signing up for mobile-pay apps, do you fully understand the different types of personal information that are being tracked when you use the app?

Yes, I make certain to read the terms and conditions

No, I do not read the terms and conditions



You are a regular user of a mobile-pay app and your provider is hacked, compromising your personal data. The issue is fully corrected, but nonetheless: how comfortable will you be in continuing to use mobile-pay apps?



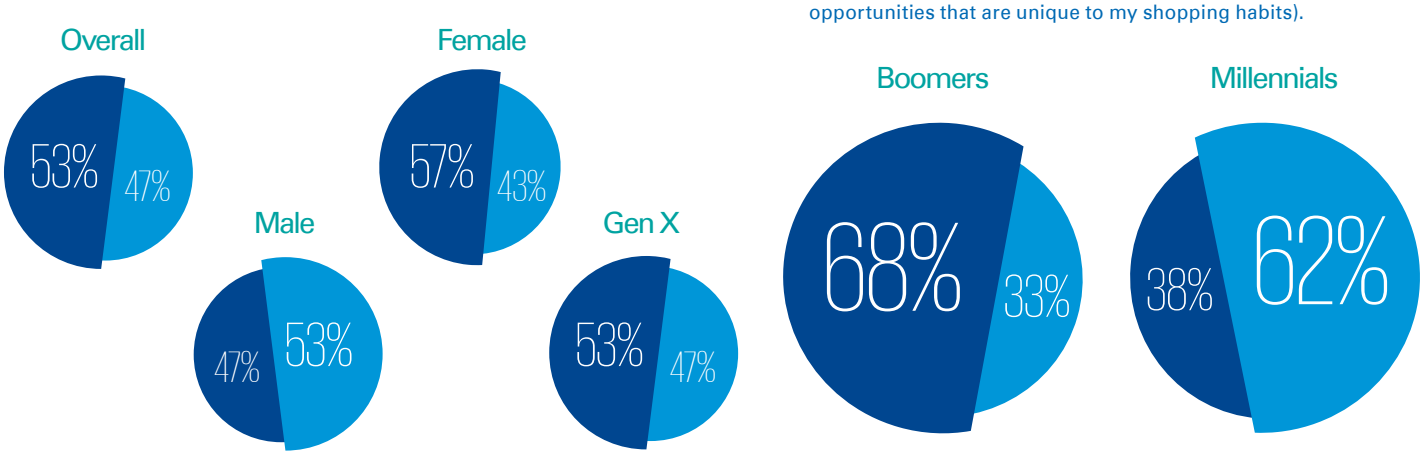
Cybersecurity: Personalisation

Which of the following statements best describes how you feel about shopper personalisation?

Boomer and millennial attitudes are polar opposites.

I don't like the idea of shopper personalisation (because I don't want my personal shopping habits and information to be collected).

I like shopper personalisation (and don't mind if my personal information is stored because it provides me with deals on opportunities that are unique to my shopping habits).



"Whether online, mobile, or in person, we see retailers moving from mere segmentation to one-to-one, omnichannel personalisation. Greater touchpoint personalisation means more historical and real-time information being captured, stored, and engaged to place the customer first. But consider the cost of a breach: on sales, on trust and brand, on customer relationships. Pursue a digital strategy by all means, but understand your business isn't merely sales, it's digital intimacy. Providing a seamless but secure customer connection is no longer a mere IT risk, but instead emerges as a strategic brand, product, and service imperative."

— Mark Larson,
KPMG's National Line of Business Leader for Consumer Markets and Global and US Sector Leader for Retail

Conclusion

Staying ahead in a never-ending struggle

In conclusion:

- The distinction between technology-focused and traditional companies is now irrelevant. Any business having products, services or customers now needs data security as a fundamental component of its tech-based offerings.
- Data, business and cybersecurity must be managed hand in hand.
- Companies need to begin thinking about cybersecurity less as a purely IT-managed risk and far more as a strategic business issue.
- Branding, loyalty, sales, overall customer relationships and business agility all hang in the balance.
- Hackers, would-be thieves or troublemakers lurking internally, and other cybersecurity insurgents will never stop trying to break in and wreak havoc. This is a never-ending state of war, with both sides continually probing the strengths and weaknesses of ever-evolving technologies.
- While this may be "old news" to IT departments, the urgency cannot be overstated. It is time for IT and the business to merge as one to manage the risk/opportunity set.
- Beyond having their reputations at stake, companies are also at risk in terms of cashflow, heightened regulatory attention, and even litigation.

The view is clear from any angle, whether looking from above or below the surface: the stakes are high. Therefore, the time is now to assess your business's threats and opportunities from the cybersecurity standpoint on all levels.

Methodology

This report is based on two separate surveys: one for businesses and another for consumers. The surveys were authored by KPMG and fielded by Forbes Insights.

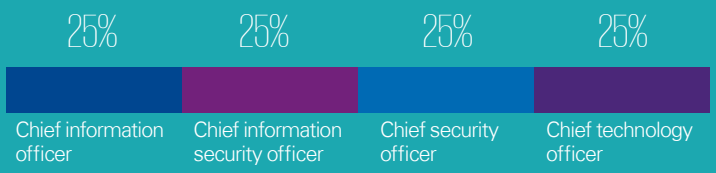
The corporate survey: demographics

The survey for corporations was completed by 403 senior cybersecurity executives all residing in the US. The titles are equally distributed between chief information officer (CIO – 25%), chief information security officer (25%), chief security officer (25%) and chief technology officer (CTO – 25%).

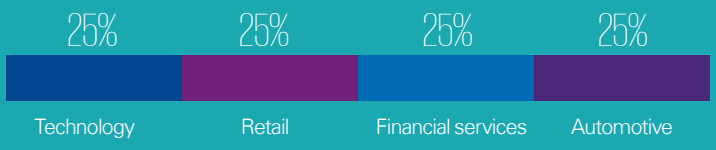
The industries represented include automotive (25%), financial services (25%), retail (26%) and technology (25%).

Revenues for those from the technology sector are well-distributed from $100 million to $20 billion — with 2% over $20 billion. Revenues from the other sectors are well-distributed from $500 million to $10 billion, with 3% over $10 billion.

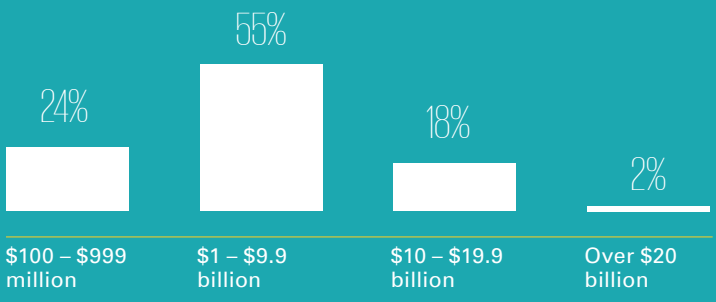
Title



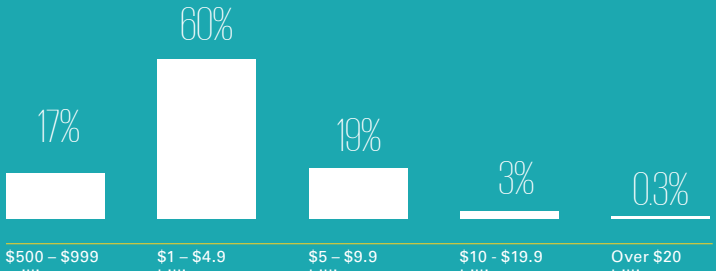
Industry



Revenue: Technology sector only



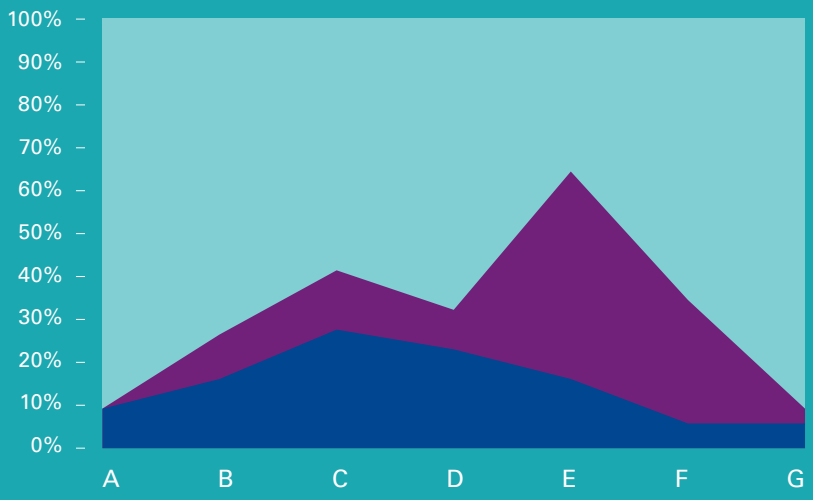
Revenue: Nontech sectors



The consumer survey: demographics

The consumer portion of the analysis is based on a survey of 750 individuals residing in the US and representing a wide and well-balanced range of income levels, education and ages (see tables). For purposes of simplification, the age groups are defined as millennials, gen X and boomers. The sample is nearly equally balanced between males (47%) and females (53%).

Household income



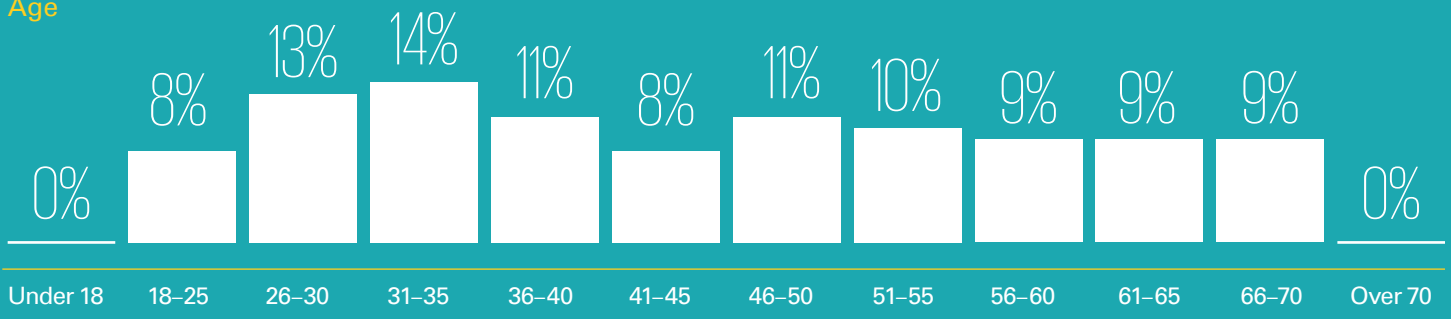
Income

A -$25,000 – $34,999
B - $35,000 – $49,999
C- $50,000 – $74,999
D- $75,000 – $99,999
E - $100,000 – $149,999
F - $150,000 – $199,000
G - $200,000 or more

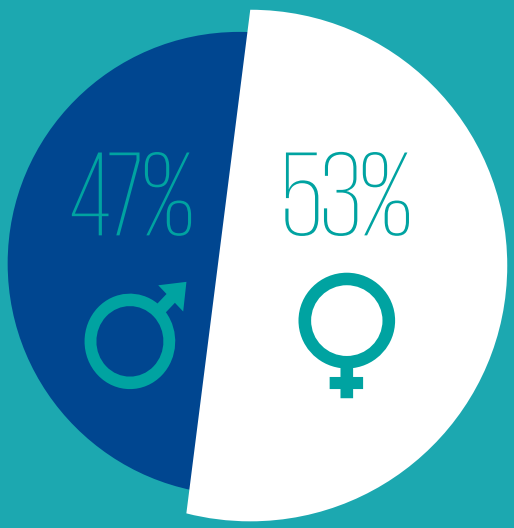
Education

Less than high school
High school graduate
Some college
Associates degree
Bachelors degree
Graduate or professional degree
PhD

Age



Gender



Other key attributes

98% have a personal checking account, savings account or credit card.

97% use a mobile phone.

98% own at least one additional piece of technology such as a tablet, PC, laptop, game system, television, etc.

94% own or lease an automobile.

97% have shopped at a big-box retailer in the past year.

Though in total 750 consumers participated in the survey, each was assigned, randomly, to only three of the six available research tracks. This results in an average sample size of 449 individuals in each track.

About KPMG

KPMG, the audit, tax, and advisory firm (www.kpmg.com/cn), is the China member firm of KPMG International Cooperative ("KPMG International"). KPMG International's member firms have 174,000 professionals, including more than 9,000 partners, in 155 countries.

About KPMG Cyber

KPMG Cyber assists global organizations in transforming their security, privacy, and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs.

Contact us

Henry Shek
Partner, IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Richard Zhang
Director, IT Advisory
KPMG China
T: +86 (21) 2212 3637
E: richard.zhang@kpmg.com

Calfen Cui
Director, IT Advisory
KPMG China
T: +86 (10) 8508 5470
E: calfen.cui@kpmg.com

www.kpmg.com/cn/cyber