KPMG

Consumer Loss Barometer

The economics of trust

kpmg.com/consumerlossbarometer

Contents

1

The economics of trust

Introduction

Trust in the time of disruption

Navigating technology disruption is now a business norm, propelling organizations to both experiment with and deploy advanced digital products and services that increasingly collect, leverage and ultimately create value from abundant amounts of data. The continuous nature of technology development, and the ability to drive customer engagement and gain performance enhancements through digital transformation, generates significant excitement at a board level — both as an opportunity to gain a competitive advantage, as well as being a catalyst for disruption. The ability to achieve agility in what is now a continuous process of transformation and innovation is fast defining success for organizations, and maintaining trust in the age of the customer is becoming a differentiator for those able to act and demonstrate an understanding of their consumer's concerns.

Consumers are a key driver in the digital transformation agenda, as digital engagement evolves and expectations rise. Successful organizations must anticipate and respond to commercial opportunities arising from consumers who increasingly demand trusted and digitally enabled experiences. Fully understanding individual consumer demands is critical to business success, and this requires the collection of a significant amount of data. To fully harness the benefits from technology, companies must better position themselves to seize opportunities arising from consumer trust agendas — agendas which have gained priority against a backdrop of new cyber threats to both organizations and the consumers who use their products.

In this new survey, our aim was to assess whether there has been a shift in consumer expectations regarding digital trust, and whether organizations are placing the consumer's security front and centre of their digital product offerings. We also explore what it takes for consumers to stay with a brand when things go wrong — and whether organizations genuinely place consumer interests first during times of crises.

Understanding the gap in perceptions of cybersecurity between consumers and the organizations that serve them is a key theme of this report. We believe that solving this gap in perceptions generates consumer trust and confidence propels business growth.

> “The needs and expectations of the consumer are becoming ever more important in shaping business decisions and are leading the discussion among organizations about their digital transformation,” *says* ***Gary Reader****, KPMG Global Head of Clients* and Markets. As customers communicate using more digital channels and hand over more data to organizations, are organizations doing enough to address their consumers' needs?”

The rise of the concerned digital consumer

As technology innovation progresses, consumers are revising upward their expectations on how organizations deliver digital products and services, and expect security as integral to their digital experience. Based on our research, it is clear that many consumers actively embrace new, personalized and user-friendly technology. However, concerns around data security are also increasing and, in many cases, consumers are uncomfortable with the way that businesses address these concerns.

Boards at a crossroads

Digital transformation is now a way of life for all organizations, but many boards appear to actively engage with only part of the transformation agenda. Most boards are significantly more comfortable with the upsides of transformation — incorporating new technology and data strategies for growth — while overlooking the potential risks associated with these.

This is reflected in our responses from security leadership. More than a third of security executives considered their organization's information-security budget inadequate. Worryingly, some security executive respondents stated that their company views information security primarily as a compliance and risk management issue, with 12 percent briefing the board on only an annual basis or less.

We believe that when cybersecurity is left out of the business value chain, a trust ecosystem is not delivered, a significant commercial opportunity is missed, and the risk for all increases. Boards should balance their responsibilities between the growth agenda with the customer trust agenda.

"Twenty-first century enterprises use technology to enable consumer engagement, realize value from intangible assets, and develop the workforce of the future," *says* ***Greg Bell****, KPMG Global Co-Leader, Cyber Security.* "But these models should be broadened to include cybersecurity as part of the investment, enabling organizations to change faster, while reducing risk."

Friction and unmet expectations

Only a handful of best-in-class businesses are fully integrating cybersecurity into their business transformation agendas from the outset, building digital products and services that meet both the functional and security expectations of consumers. The remainder typically attempt to retrofit security endeavors to already established or near-complete transformation outcomes. Friction is inevitably created when security requirements are added at a late stage, delaying or even halting delivery of digital transformation objectives.

If boards and business leaders do not fully embed cyber into their business strategy at the outset, there is a risk that their commercial strategy will become fragmented, with only certain consumer expectations being met.

"The role of the CISO has evolved. CISOs are now pivotal in supporting their organizations' growth ambitions, largely through delivering trust in the digital products and services," *says* ***Akhilesh Tuteja****, KPMG Global Co-Leader, Cyber Security*. Indeed, the survey shows that CISOs regard themselves as integral to their organizations' growth, but remain insufficiently integrated into the business transformation agenda. "Still, there is cause for optimism; many CISOs feel that they receive the support of their organizations, with adequate budgets and levels of investment," he says. As consumer trust becomes increasingly critical to commercial success, it will become more and more important for cybersecurity to be treated as a board-level investment priority, and be seen as a key enabler of business growth.

Retaining consumer trust in times of crisis

Trust is crucial to attracting and retaining consumers, but this is critically tested when incidents occur. KPMG's 2018 Global CEO Outlook found that half of chief executive officers believe that it is purely a matter of time before their organization experiences a cyber incident. But if such an event is handled sensitively and in a way that reinforces consumer trust, we have found that this can actually strengthen the trust ecosystem and improve a company's ability to retain consumers.

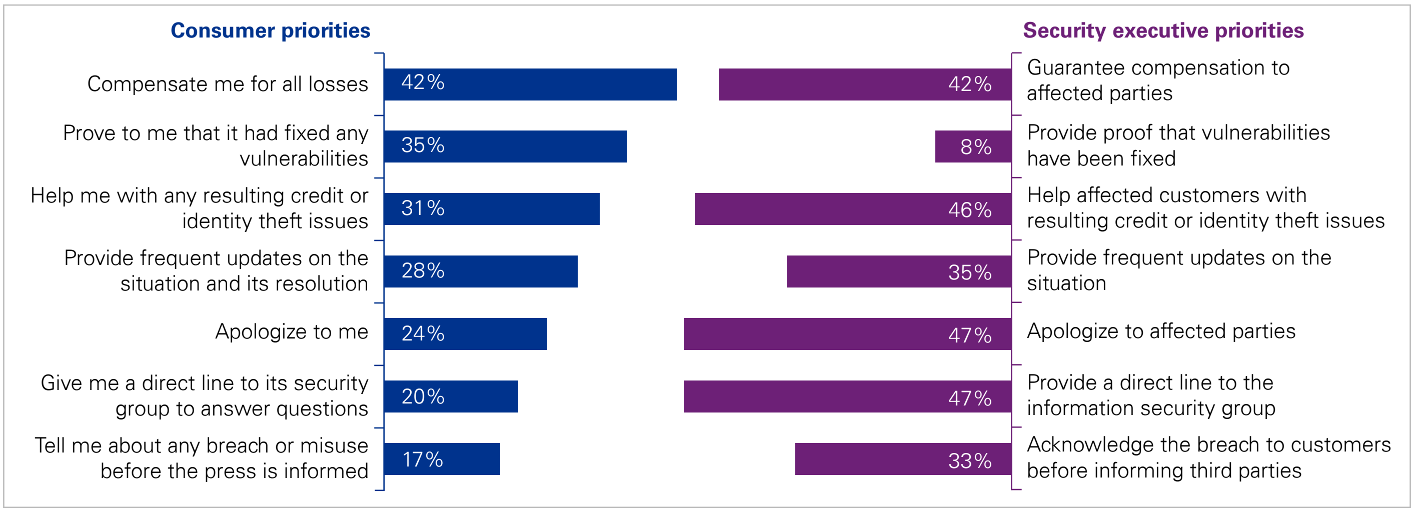
The survey identified a significant mismatch between the priorities of security executives and consumers in the event of a breach. More than a third of consumers would want the company to prove it had fixed the issue; however, only eight percent of security executives would prioritize providing such proof. Conversely, only 24 percent of consumers would prioritize receiving an apology, whereas about half the security executives surveyed would prioritize this.

We believe that, as consumer expectations around security rise, the role of the security organization will expand from protecting the organization's core technology-enabled processes and add to the value proposition of digital products and services. It is important, then, for security leadership to understand the needs of the end-consumer, and move from being a back-office function to a core element of the consumer experience.

Do security professionals really know what consumers want?

Consumer priorities: *If there were a loss of funds from your financial account or theft or misuse of your personal data due to a security breach, what would your financial service provider need to do to keep you as a customer? Select all that apply.*

Security executive priorities: *What steps does your organization typically take to respond to customers and other parties once a breach is discovered and remediated? Select the top three.*



Source: Consumer Loss Barometer. Economics of trust. 2019.

Customer-centric incident response

Companies should plan ahead, by thinking through the appropriate response to these concerns before an incident occurs. The central question that security professionals need to ask themselves is how do their actions contribute to the trust ecosystem? Companies that are better prepared will likely have a good chance of retaining customers when an incident occurs.

Responding to major cyber crises requires actions across an organization, from technical responders right up to the board and executive leadership. Only through an orchestrated and organization-wide response can meaningful results and actions be delivered.

It is critical that confidence is maintained — especially when it comes to external stakeholders. Security professionals and incident responders are crucial to this, and they require the support of the board and all customer-facing employees.

"Understanding consumer expectations in the event of a crisis, and planning how to orchestrate a response, will improve resilience and help regain the trust of those affected." *says **Paul Taylor**, Partner, Cyber Security, KPMG in the UK.*

2 The consumer view

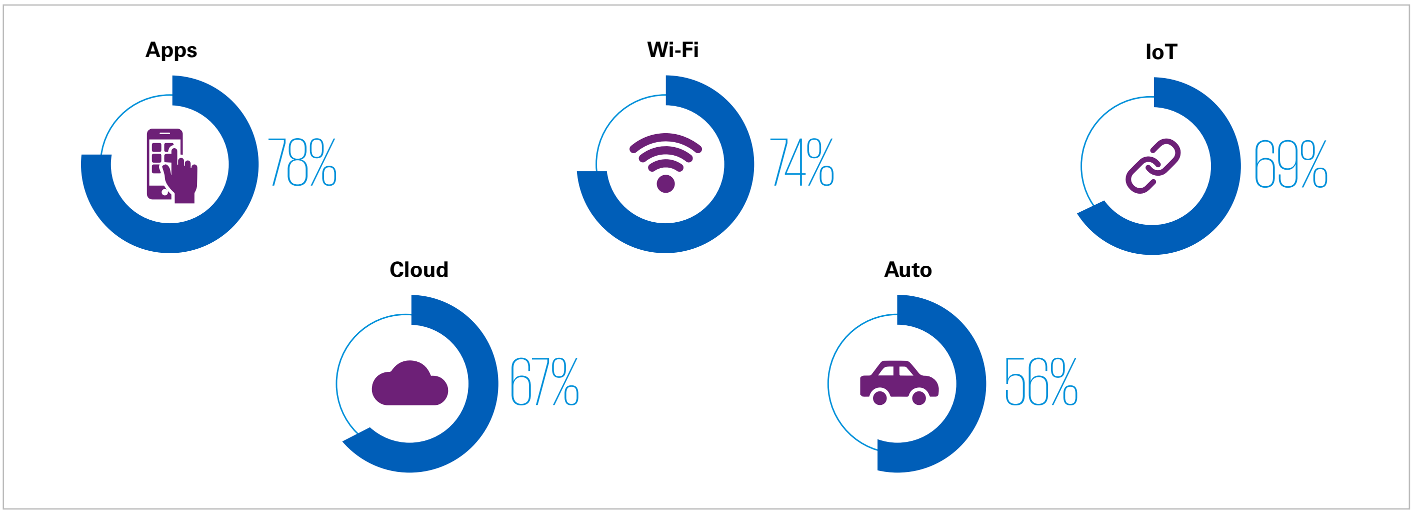
Consumers are increasingly aware and concerned of cybersecurity risks

Similar to executives in the boardroom, consumers are embracing the role technology can play in adding value to day-to-day interactions — both with companies and with one another. From a consumer point of view, technology change and adoption is already or fast becoming a way of life, simplifying and enhancing how consumers connect.

And similar to executives, consumers are also aware that the upside of technology advancement has a potential downside. Our survey found that the majority of consumer respondents had a high level of concern when it comes to using technology, with a clear correlation between the maturity or familiarity of a technology and the level of concern consumers expressed about that technology.

At a minimum, we can draw the conclusion that organizations are not doing enough to demonstrate the security around digital products and services. We also believe that those who can cross the divide between consumer expectations and concerns can gain a competitive advantage in the fight for the consumer, making the economics of trust a key strategic differentiator.

Percentage of respondents who are concerned about the technology being compromised



Source: Consumer Loss Barometer. Economics of trust. 2019.

Apps and Wi-Fi are two technologies that consumers are most concerned about being compromised and are most in use by the average consumer. Apps in particular receive a large amount of focus from organizations when delivering digital customer engagement models. While connected automobiles featured lower on the concern radar, the relatively lower maturity and full-scale adoption of this technology may be a factor, with respondents recognizing that this will be an area of concern in the future (as explored later in this report).

"Consumers are rightly concerned about data breaches; we are constantly reading in the news about incidents impacting millions, with leaked personal information including passwords, activity logs, and financial records," *says* ***Akhilesh Tuteja****, KPMG Global Co-Leader, Cyber Security.* "Consumers are worried about how these breaches will affect them personally and are less concerned about the impact of the breach on the organization that is hacked. As organizations continue their transformation journeys, those that are able to address their consumers' concerns can have a competitive edge."

The economics of trust — Financial services

Digital banking has become the norm, both in developed and emerging economies, with more than two-thirds of consumers globally using digital banking platforms and 515 million customers opening a bank account through a mobile money provider.

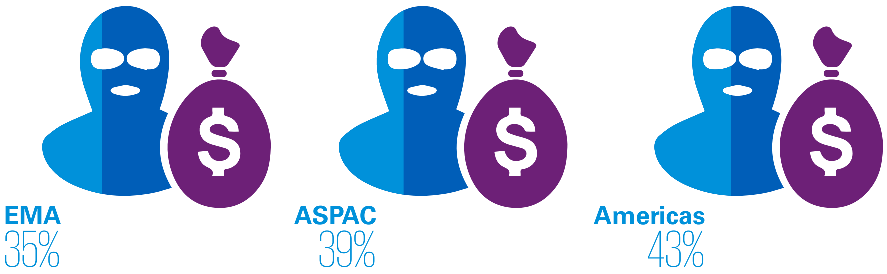
The opportunities presented by digital financial services are clear and, we believe, already proven. In established markets, financial services organizations are able to engage directly with consumers, increase their speed to market, tailor their products and services to their consumer needs, and reduce or contain their operational costs. In emerging markets, digital banks have the ability to reach previously unbanked consumers without having to establish a major physical presence, thereby eliminating significant capital investment requirements. Enabling this, however, requires a high level of trust from the consumer.

An additional challenge that financial institutions face is that financial information and the trust ecosystem for consumers often includes third parties — product and service providers who capture and pass financial information through to complete transactions — and the complexity of this ecosystem is growing as open banking and other initiatives become mainstream.

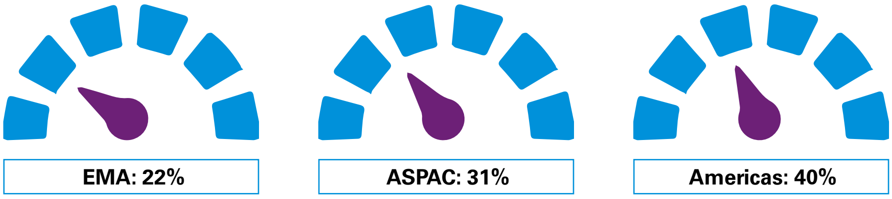
The attractiveness of this information to attackers is clear, with 37 percent of consumer respondents globally indicating that they have had their financial information compromised, including more than a third of respondents in LATAM and North America having had their financial information stolen. This context provides a challenging environment for financial institutions, which need to operate and retain consumer trust while pursuing their digital transformation agendas.

There is also a clear correlation between the relative maturity of the digital transformation agenda and the percentage of consumers who have had their financial information compromised within a region. From this we can infer that the risk to consumers intensifies as digital transformation progresses.

Percentage of respondents who have had their financial information compromised, by region



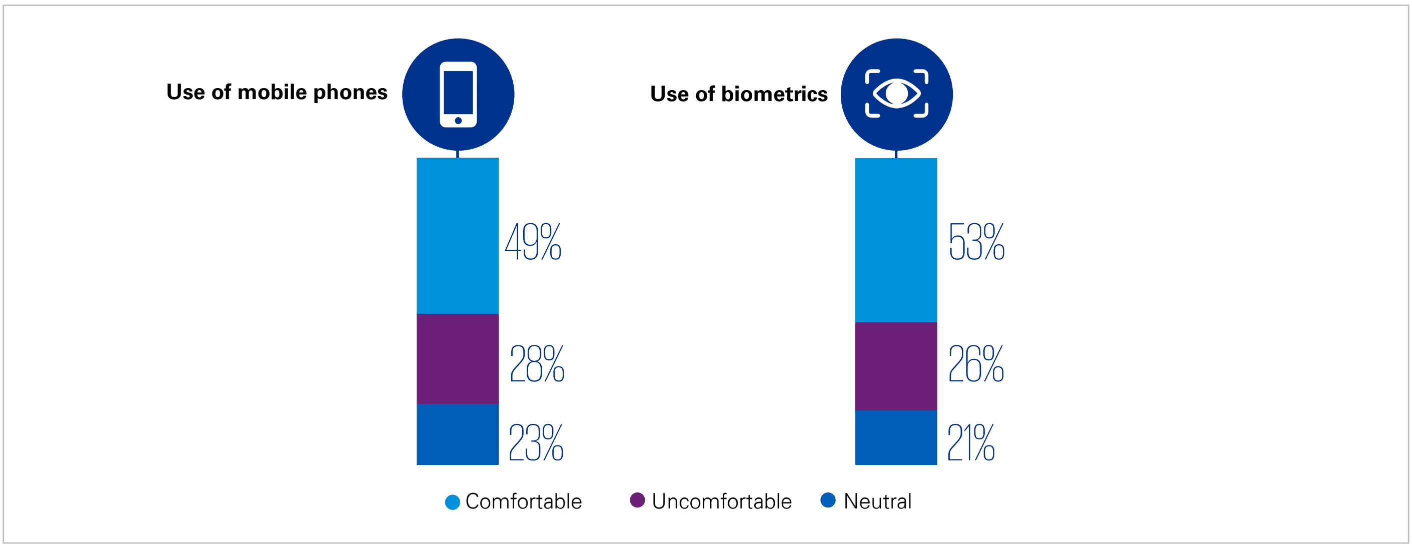
Percentage of security executive respondents who indicated that their digital transformation programs were 'advanced' or 'mature', per region



Source: Consumer Loss Barometer. Economics of trust. 2019.

> "Having served some of the largest global financial institutions in the world, I have experienced first-hand how the complexity and scale of organizations makes it challenging to easily re-design data security strategies. To achieve a holistic data security strategy — spanning business, technology and multiple security layers — requires strong board engagement and real support. When done successfully, this can truly generate growth through enhanced alignment and agility."
>
> ***Bia Bedri***
>
> *Banking and Capital Markets Cyber Leader, KPMG in the UK*

Making the case for change

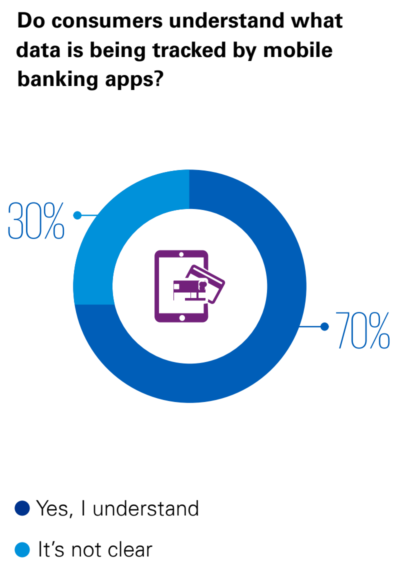


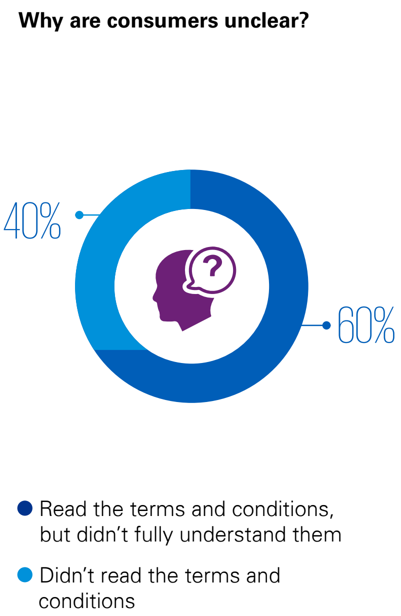
Source: Consumer Loss Barometer. Economics of trust. 2019.

Despite the popularity of digital banking, financial institutions have a large base of users across all age groups who are not comfortable with digital enablers, such as mobile phones (28 percent) and biometric authentication (26 percent).

Financial institutions should therefore do more to explain the benefits of digital enablers and show that they understand customers' concerns, especially as they become custodians of ever-increasing amounts of data. For example, banks need to do a better job explaining to consumers the advantages of biometric authentication over passwords.

A focus on the fine print





When it comes to their own digital products and services, financial institutions can build trust through educational programs that enable consumers to better understand what data is being tracked and how it is being used. Consumers are likely to understand that financial services organizations have a right to access financial information for activities relating to safeguarding their personal financial assets, such as fraud monitoring. However, behavioral analysis that is not for this purpose, such as for the purpose of targeted product marketing, may cross the trust boundary.

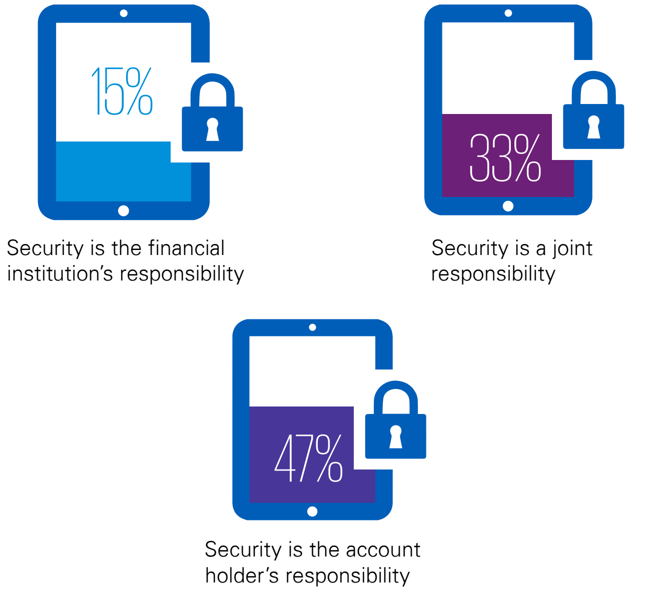
Source: Consumer Loss Barometer. Economics of trust. 2019.

Shouldering responsibility

Almost half of consumers believe that their financial institution should have full or joint authority for ensuring that mobile devices used for banking are secured. Whether or not financial institutions regard it as their responsibility, they need to show they take the security of their customer's information seriously, both in their clients' interactions with them and their clients' broader security needs.

"Financial institutions face a real challenge in keeping up with consumer expectations around security," *says* ***Judd Caplain***, *Head of Global Banking and Capital Markets*. "A handful of key players are getting this right; they do so by seamlessly integrating agile security into their digital transformation agenda, while recognizing that the agenda itself is in constant flux. They then make their efforts demonstrable to their customers, for example, by providing easy access to cyber security awareness and fraud monitoring."

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



Source: Consumer Loss Barometer. Economics of trust. 2019.

Playing for customer stakes

When surveying consumer respondents, only 1.2 percent of respondents would definitely change their financial services provider if their financial information was breached. Conversely, two percent of respondents would definitely remain with their financial services provider after a breach, although more than half of these would remain as it is too burdensome to switch. The remaining 96.8 percent of respondents would be willing to remain with their financial services provider, provided the organization took the appropriate actions to address their concerns.

This shows that consumers accept the reality that cyberattacks cannot be completely avoided, but they do expect a swift and effective response to a breach.

Our survey identified that many consumers would be willing to stay with an organization following a breach if the organization met their expectations and focused on their priorities. The top priorities for consumers in the event of a breach are being compensated for all losses incurred, receiving proof that vulnerabilities had been fixed, and receiving assistance with any resulting credit or identity theft issues.

The economics of trust – Cloud and connected devices

Is connected device security a cost, an investment, or a differentiator?

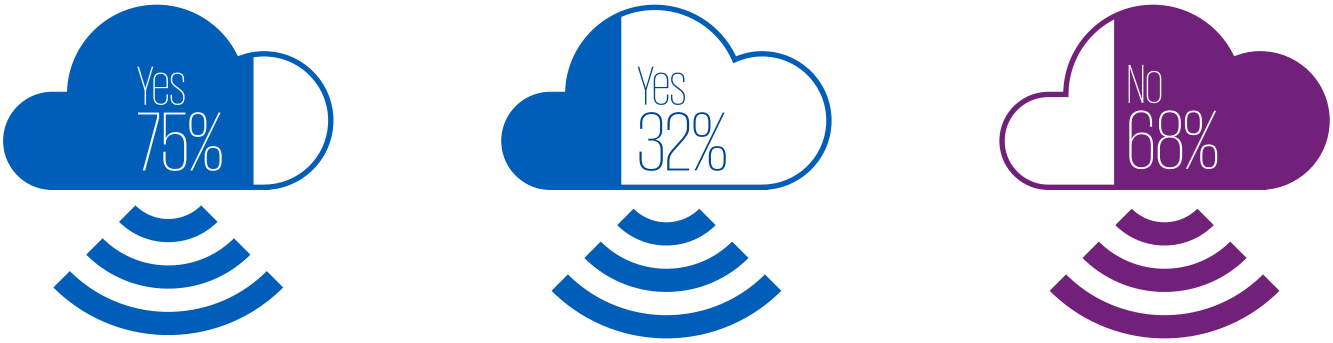
During our survey, three-quarters of consumers said they expected additional security and privacy to be designed into their connected devices. But this does not necessarily translate into action: only 32 percent limited the use of such devices and again only 32 percent were willing to pay a higher price for more secure devices. This creates a challenge for device manufacturers, with consumers expecting a high level of data security, but not necessarily being prepared to pay for it.

Businesses must acknowledge and exploit the upside to strong security: a trust economy that can propel business growth. Investing in device security as a matter of routine hygiene reduces consumer concern and pays off through increased sales or, just as importantly, creates brand loyalty once issues hit similar devices on the market. This is an important differentiator given the growth projections of connected devices.

Should there be additional levels of privacy and security embedded within the design of new types of 'connected' devices?

Have you limited the use of new types of 'connected' devices due to security or privacy concerns?

Would you consider paying for additional levels of security for some of the new types of 'connected' devices that you use?



Source: Consumer Loss Barometer. Economics of trust. 2019.

The number of IoT devices worldwide totaled 7 billion in 2018 (excluding smartphones, tablets and laptops), and this is expected to triple by 2022. "The proliferation of connected and IoT devices will have a cross-sector impact on areas around data security and privacy. In response to this, regulators will need to establish mandatory data security requirements," *says* ***Atul Gupta****, IT Advisory Leader, KPMG in India*. "This also presents an opportunity for organizations to build a trusted environment and position it as a selling point. Trust then becomes a differentiator in consumers' buying decisions."

Cloud platforms

Are social media platforms inherently distrusted?

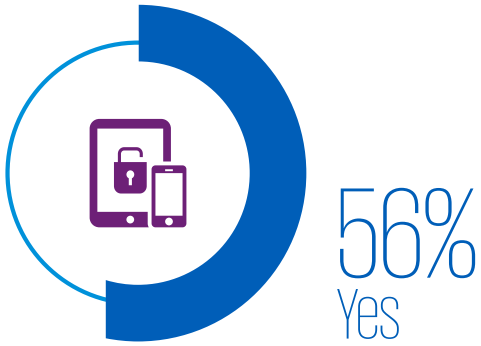
As part of our survey, we found that over half of users are limiting the amount of personal data stored online. For social media and other platforms where content delivery is driven by user data (to provide content and, ultimately, personalized marketing platforms), there is a risk that the platforms become unable to obtain the information needed to drive their algorithms to maximum advantage.

From another lens, these platforms also need to safeguard their own content delivery strategies, algorithms and ultimately the content delivered to the end user. The ability to 'weaponize' content delivery platforms to sway public opinion and debate is gaining prominence in the media, with organizations facing a double impact on their trust equation.

In the short term, however, it seems that there is some respite — with consumers being slightly less likely to switch or disable their social media accounts when they feel that their privacy is being infringed upon (46 percent of respondents would consider doing this).

Longer term, however, social media and cloud platforms need to consider how they can regain the trust of the consumer, or face disruption from either emerging players who can, or from the regulators who may increasingly act on behalf of the consumer.

Are you limiting the amount of data you store on cloud/social media platforms due to security and privacy concerns?



Source: Consumer Loss Barometer. Economics of trust. 2019.

> "Organizations from all sectors are deploying data-driven strategies supported by technology innovation to increase agility and speed to market. A handful of front-footed organizations are also using these strategies to get ahead of regulatory developments and using this to their advantage: getting ahead of the curve and proactively demonstrating strong care for managing security and privacy."
>
> ***Jitendra Sharma***
> *Global Head of Risk Consulting, KPMG International*

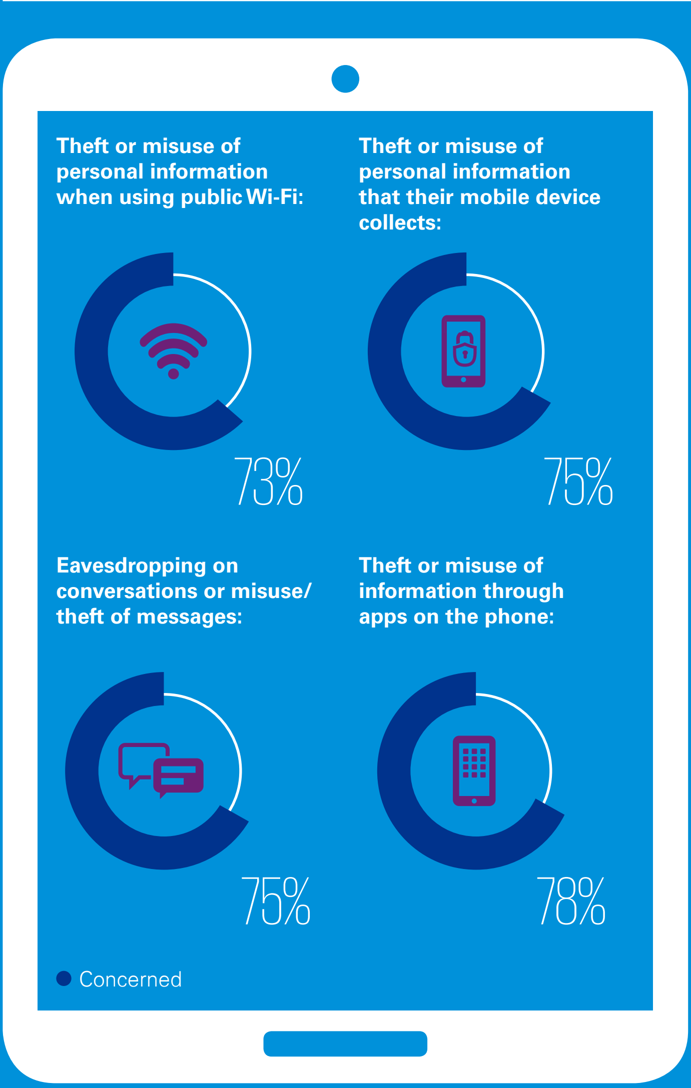
The economics of trust — Mobile

The backbone of the trust economy

As a core enabler of the digital economy, mobile device manufacturers and network operators sit at the crux of the trust economy — needing not only to create trust in the security of their own products and services, but also to create trusted channels and platforms that enable consumers to take advantage of digital products and services from almost every other industry.

As part of our survey, however, we found the level of concern among consumers to be very high — with, on average, three-quarters of consumers concerned about their devices, their operators, their network connections or the software they had on their phone.

Top of mind for mobile consumers



Source: Consumer Loss Barometer. Economics of trust. 2019.

Consumers have significant concerns around the security implications of mobile technology. They are aware of the risks, which impacts on purchasing and usage trends. Mobile providers that are successful in managing consumer concerns around security, not just of their own products and services but also of their broader digital economy, can gain a competitive advantage.

Concern is growing around the consequences of using mobile technology as consumers are becoming increasingly dependent on such technology. Similarly, organized crime has recognized the growing importance of mobile technology to our global economy and has expanded its efforts to target those technologies, while providers seek to improve security in response.

Consumers hold communication providers to a high standard

As part of our survey, we found that consumers are vocal about changing their providers when their personal data is affected, whether this is due to a breach through an external attack or because of internal misuse. The number of consumers who would consider changing providers increases when the mobile provider misuses data, compared to when a mobile provider is hacked.

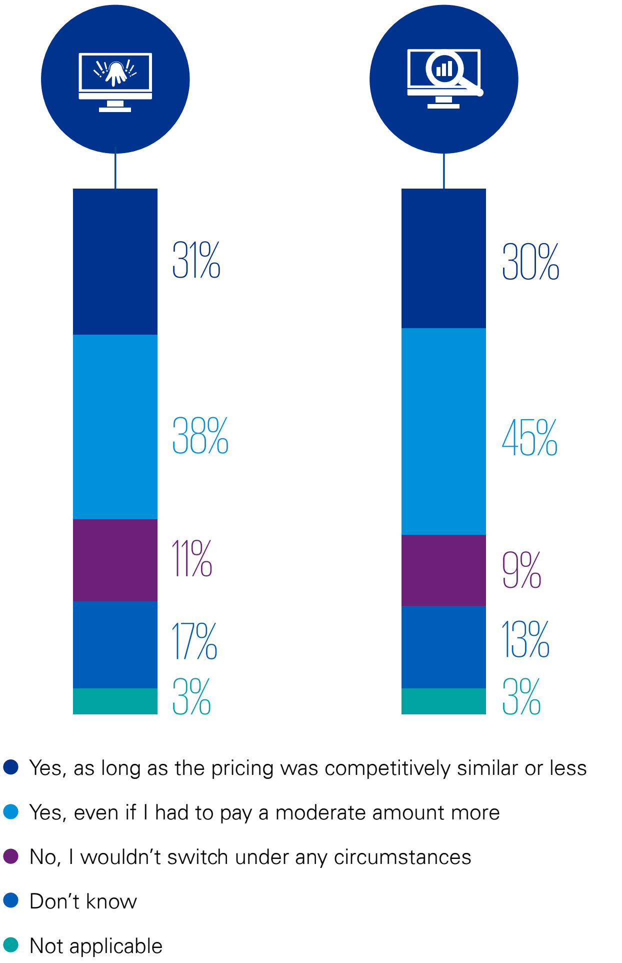
While this may not necessarily translate into action today as consumers face prohibitive contract exit fees, it could cause problems in the future should regulators or the market demand easier switching options for consumers in the mobile communications industry.

> "The economic and social impact of mobile device manufacturers and network providers goes far beyond their own products and services. They form the basis for much of our personal and working digital lives," *says* ***Alex Holt****, Global Head of Media & Telecommunications.* "These organizations can differentiate themselves by building consumer trust in the digital channels for sectors such as healthcare and banking, not just in the mobile products and services they provide. In doing so, they can increase take-up of new services and generate new revenue streams."

In which circumstances would concerns about data security or privacy prompt you to switch mobile service providers? Would pricing influence your decision?

If you learned that your mobile service provider had been hacked, compromising personal data that had been accumulated, would you switch to another provider that promised to limit or end its collection of such data?

If you learned that your mobile service provider was misusing or selling data it had accumulated on you, would you switch to another provider that refrained from these practices?



Source: Consumer Loss Barometer. Economics of trust. 2019.

The economics of trust — Automotive

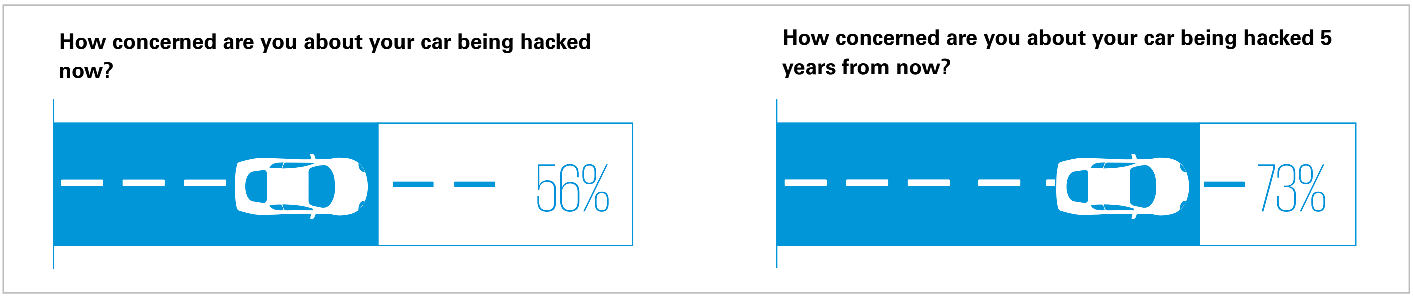
> "Data & cybersecurity, followed directly by total cost of ownership, are the most important purchasing criteria. Whether purchasing a vehicle or using a mobility service over the next 5 years, nearly 60 percent of executives absolutely agree that companies that do not focus on data and cybersecurity are at extremely high risk of sacrificing their brand reputation and not providing real value in their data usage," *says* ***Dieter Becker****, Global Head of Automotive*. "In this context, it will be even more important to create a secure digital environment with seamless connectivity and extra features that build maximum customer trust."

Change in the fast lane

Few products are facing the same level of technology disruption as automobiles, with the consumer product no longer being a combination of hardware and mechanics, but moving to an overall experience that encompasses IoT devices, data processing, automation, connectivity, software, and multiple service providers that come together under a single brand. With the additional context of technology players entering this market with alternate mobility models, traditional motoring brands are facing the daunting necessity of rapid digital transformation.

Consumers recognize how the automobile industry is transforming to become increasingly digitized, and hence vulnerable to being hacked, with the levels of concern about cyber safety rising rapidly over a 5-year horizon.

Linking cybersecurity to the safety aspect of vehicles, especially as real-world safety implications become an imperative, can be a brand differentiating value proposition in the future, similar to the safety ratings of new car assessment programs today.



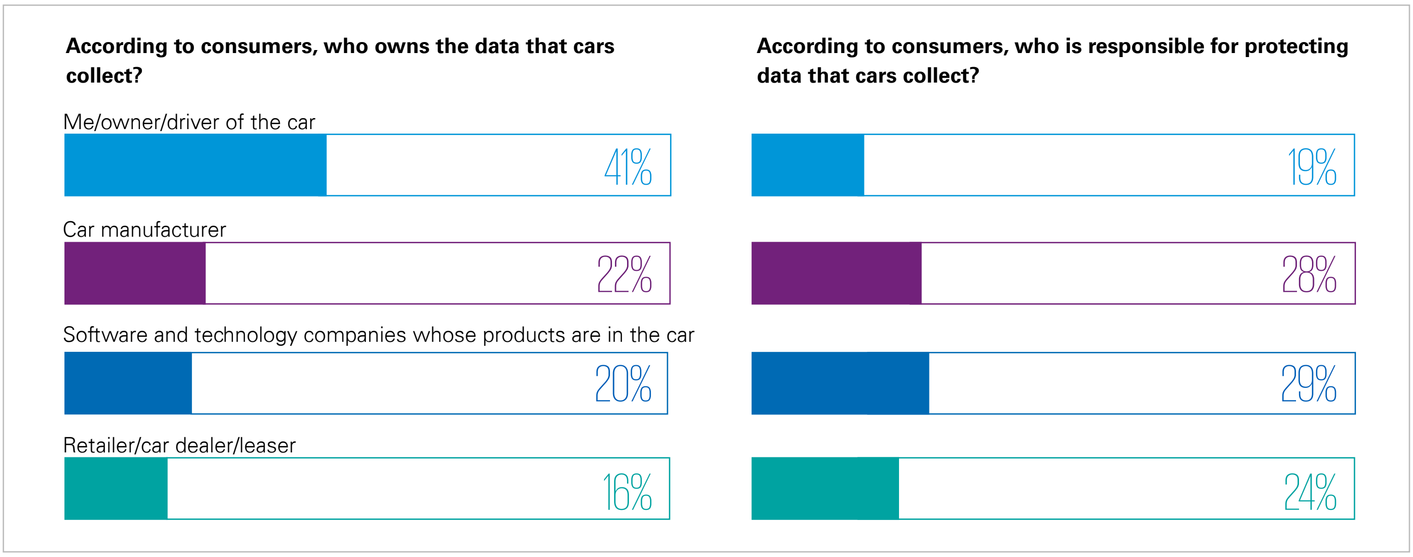
How concerned are you about your car being hacked now?

How concerned are you about your car being hacked 5 years from now?

Source: Consumer Loss Barometer. Economics of trust. 2019.

Responsibility in an ever-growing, connected network

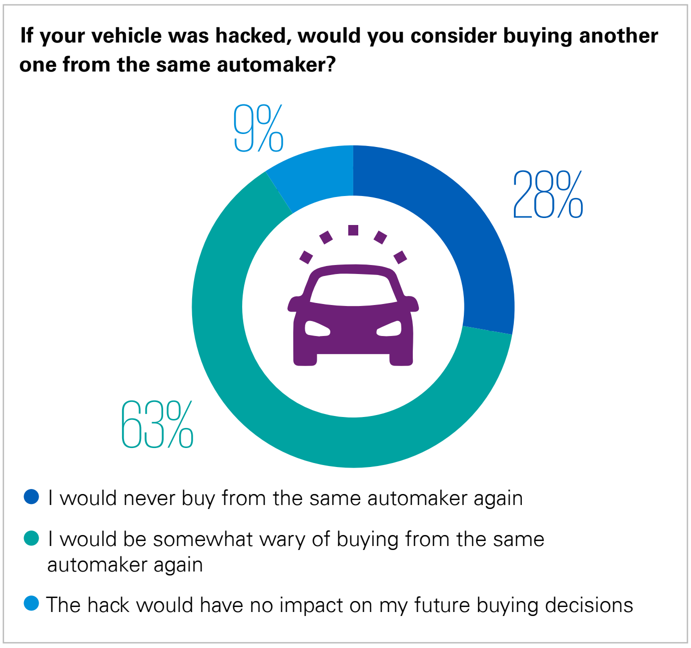
To complicate matters, car manufacturers are being held responsible for securing customers' personal and vehicle data. This is in parallel to the fact that most consumers feel that they own the data collected by cars. Consumers feel that they entrust the car manufacturer with their personal data and that they and the company share responsibility for its protection. For a car manufacturer to succeed, they need to ensure trust in their cars' data security. Automakers are being held accountable for trust in a complex ecosystem — comprising dealers, software vendors, hardware vendors, telecommunications providers and, ultimately, consumers.



Source: Consumer Loss Barometer. Economics of trust. 2019.

The impact on brand loyalty

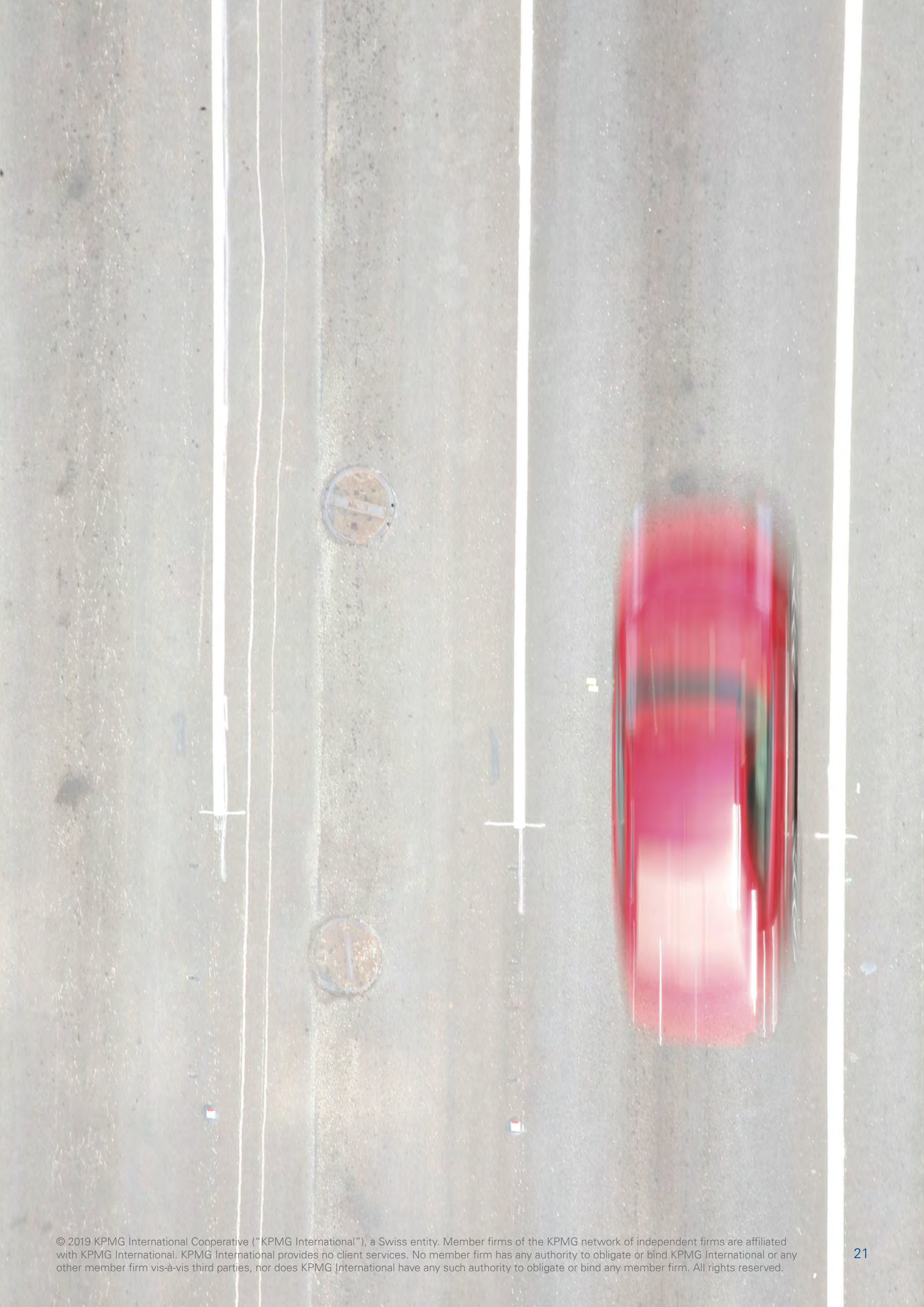
Twenty-eight percent of people indicate that they would never buy from the same automaker again if their vehicle was hacked, with another 63 percent indicating that they would be wary. This is significant — a mishandled breach could have a major impact on repeat sales, impacting an industry where brand loyalty used to rely on mechanics and a relatively low technology-based driving experience.



Source: Consumer Loss Barometer. Economics of trust. 2019.

Real-world consequences

"The data security of an automobile goes much further than the vehicle assembler," *says* ***Marko Vogel****, Cyber Security Leader, KPMG in Germany.* "Each piece of hardware, software and network architecture needs to be considered in its entirety, including the expanding ecosystem that encompasses it. This is not just about trust in the brand, but about something that lies at the heart of consumer protection — protecting consumers' lives and those around them, as well as their data."



The economics of trust — Retail

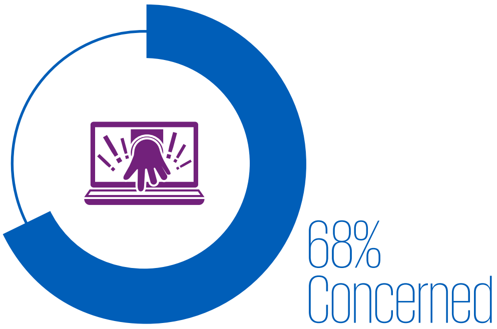
> “For competitive retailers, collecting and using personal and transactional data is critical to understanding, targeting and serving their customers — but it comes with inherent risk. Data is an asset that, mishandled, can become a liability that damages a brand and destroys trust”, *says* ***Willy Kruh****, Global Chair, Consumer & Retail*. “Furthermore, the high volume of payment and other personal information that retailers collect from their customers make them a particularly attractive target for cybercriminals.
>
> “However, despite the damage that hackers can inflict upon retailers and customers alike, customers are in fact more concerned about the potential misuse of their data by the retailers themselves. In this changing landscape, companies need to look beyond such concepts as permissions and consent, and recognize data privacy is far more than a compliance-led, box-ticking exercise. It needs to be transparent and allow for customers to have full control over how and where their data is being used.”

Consumer trust is against the retailer

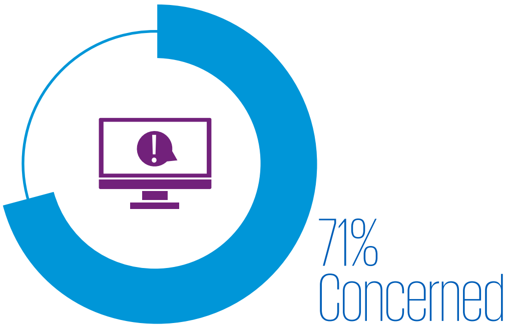
An alarming statistic that emerged when polling consumers is that there is more concern about retailers misusing personal information than information being taken by external hackers. Companies need to take this concern extremely seriously because understanding consumers and their behaviors is critical to delivering a differentiated experience.

An indispensable source of growth is to understand consumers, both what they are buying and where, and to use this data to drive sales and manage the supply chain. This helps create a lean organization designed to withstand competition and disruption from new market entrants. With shopper personalization becoming a key tactic to differentiate a shopper’s experience and increase sales, retailers need to consider the fine balance between ‘creepy’ and ‘cool’. The focal question needs to be: how far can they go in analyzing consumer data without it feeling intrusive or manipulative?

How concerned are you that a major retailer you buy from may be hacked?



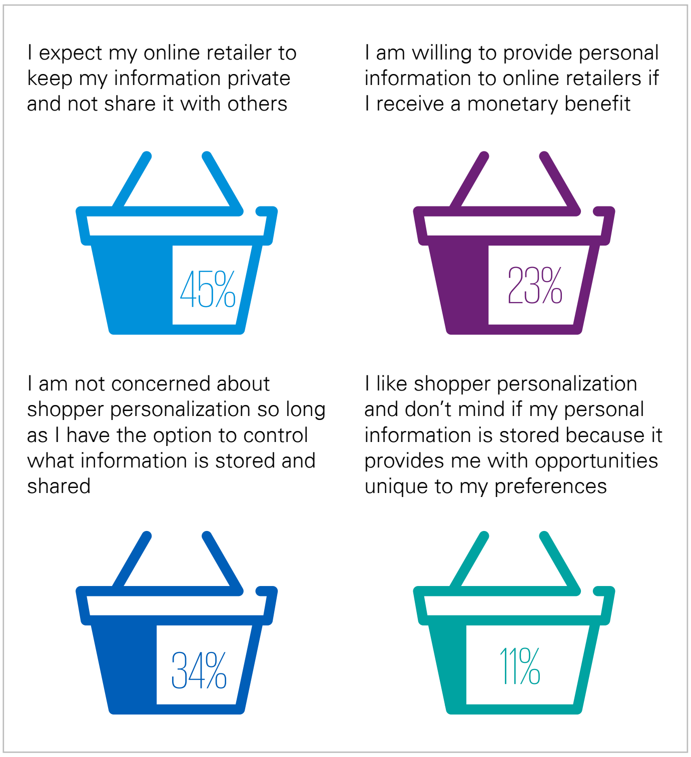
How concerned are you that a retailer will misuse or improperly distribute your information?



Source: Consumer Loss Barometer. Economics of trust. 2019.

Shopper personalization

Consumers were asked under what circumstances they value or are willing to have their data used for shopper personalization. Overwhelmingly, respondents expect a level of control or direct benefit if retailers are going to engage in personalization practices.



I expect my online retailer to keep my information private and not share it with others

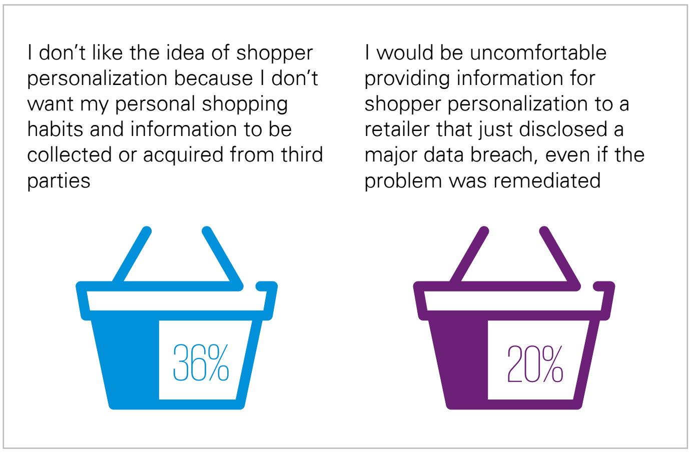
I am willing to provide personal information to online retailers if I receive a monetary benefit

I am not concerned about shopper personalization so long as I have the option to control what information is stored and shared

I like shopper personalization and don't mind if my personal information is stored because it provides me with opportunities unique to my preferences

Source: Consumer Loss Barometer. Economics of trust. 2019.

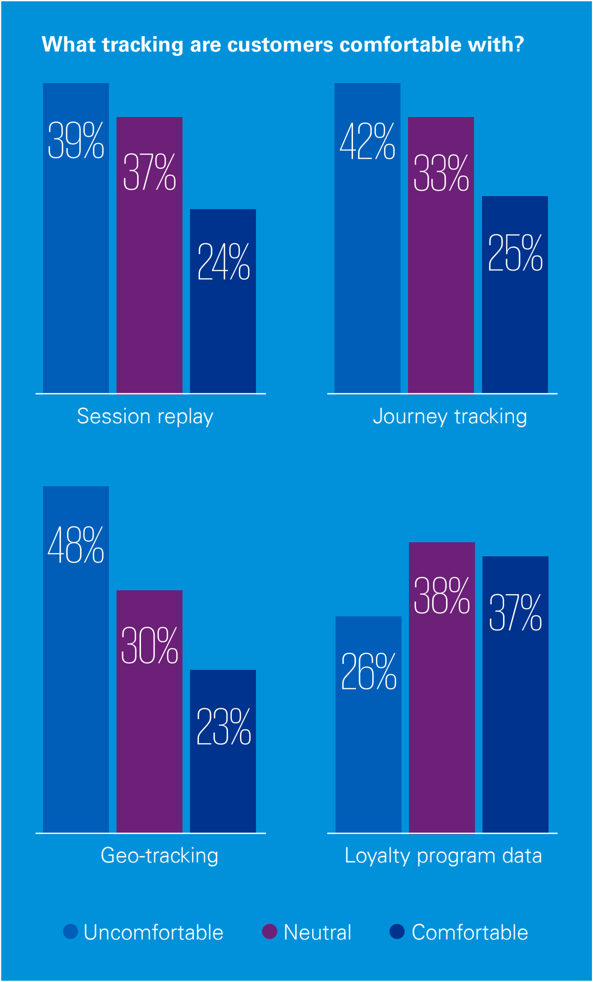
Similarly, we asked consumers what they disliked about the practice of collecting data for shopper personalization. Interestingly, consumers are more concerned about retailers sharing user information with third parties than unauthorized hacking. This reinforces the inherent distrust in the sector, which needs to be addressed by retailers as the fight for the consumer wallet and margins becomes more intense.



I don't like the idea of shopper personalization because I don't want my personal shopping habits and information to be collected or acquired from third parties

I would be uncomfortable providing information for shopper personalization to a retailer that just disclosed a major data breach, even if the problem was remediated

Source: Consumer Loss Barometer. Economics of trust. 2019.



What tracking are customers comfortable with?

Source: Consumer Loss Barometer. Economics of trust. 2019.

We further explored with our consumer respondents which techniques, specifically, they were comfortable with. By far, consumers were most comfortable with loyalty program information, and least comfortable with geo-tracking. Loyalty programs are fairly familiar to consumers, which may explain consumer's relative comfort level. The physical aspect of knowing a person's geographic location may, however, increase the 'creepy' factor of geo-tracking, with eerie similarities to 'big brother' theories, and may be seen to be crossing the line with regards to intruding on a person's privacy.

3

The security executive view

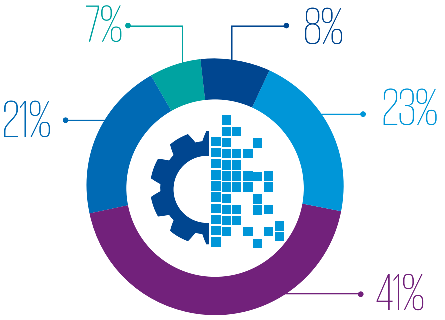
The only constant now is change

Digital transformation is now a way of life for all organizations: every organization we surveyed is on a journey to create additional business value from data and technology and create agility in their business's core operations. The scale and pace of technology evolution, however, means that organizations find themselves constantly integrating data and technology to create new sources of value and the process of transformation is now continuous.

These transformation activities are being led by executive leadership, not IT, as reflected in KPMG's 2018 Global CEO Outlook survey. Our research found that corporate leaders across industries are taking personal ownership of driving digital transformation, with 72 percent of CEOs saying they are ready to lead a radical organizational change.

The majority of our survey participants stated that they were in the intermediate stage of their digital transformation journey, with those in the technology and telecommunications industries further along their journeys than financial services, retail or auto manufacturers.

Current level of digital transformation



- ● **Stage 1** — Starting (developing and starting transformation journey)
- ● **Stage 2** — Early (process in early implementation)
- ● **Stage 3** — Intermediate (halfway through implementation)
- ● **Stage 4** — Mature (three-quarters of the way through implementation)
- ● **Stage 5** — Advanced (implementation generally completed)

Source: Consumer Loss Barometer. Economics of trust. 2019.

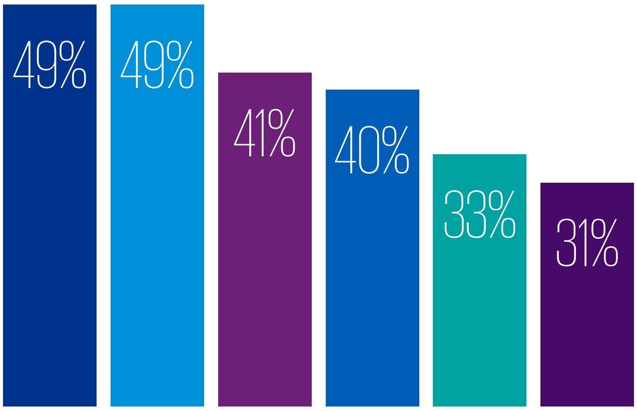
Are security functions changing at the speed of business?

As digital transformation becomes the norm and becomes a business imperative, the role of the cybersecurity function needs to change accordingly, to enable agile adoption, experimentation and implementation of technology. Cybersecurity functions that remain as reactive or compliance — based function focused on established IT and processes will be left behind in the transformation agenda. We believe that organizations that entrench cybersecurity into their digital innovation and customer-centric functions, with a mandate to enable speed and agility, can be able to bridge the cybersecurity gap between consumers and the organizations that serve them. This will help generate consumer trust and propel business growth.

Encouragingly, the potential opportunity for cybersecurity to add value to business objectives was shared by our security leadership survey respondents, with securing customer engagement and supporting digital and business transformation agendas being the top opportunities for cybersecurity.

For financial services and retail, securing consumer engagement was the top way in which cybersecurity could support organizational growth. These industries are consumer-focused, and consumers in these markets have many options to choose from. Consumer engagement was, however, a consistent high priority opportunity for cybersecurity across all the industries we surveyed.

We asked respondents how cybersecurity could enable growth:

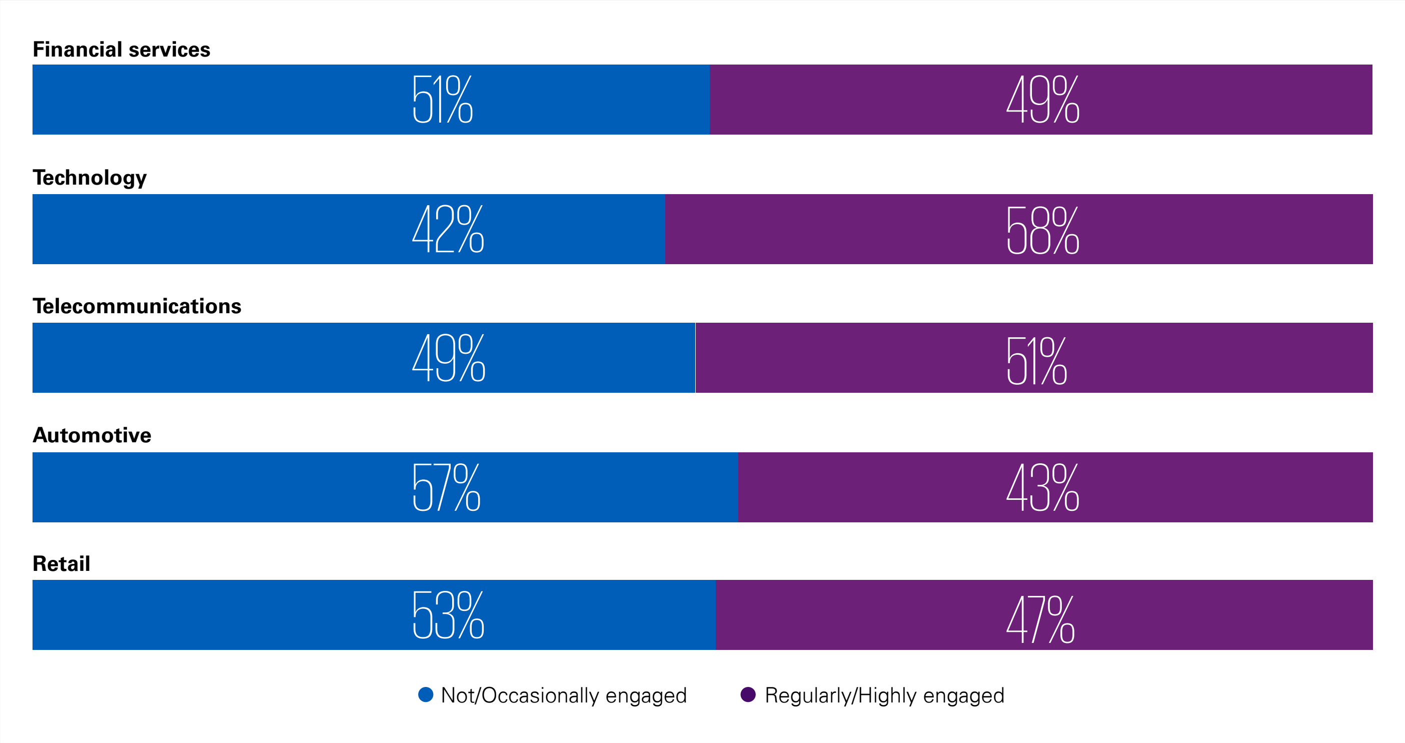


- ● Secure customer engagement
- ● Support digital transformation and business priorities
- ● Maintain cyber hygiene to operate at peak efficiency
- ● Enable speed to market
- ● Demonstrate cyber agility and resiliency
- ● Achieve a competitive advantage

Source: Consumer Loss Barometer. Economics of trust. 2019.

Cybersecurity in the digital transformation agenda

While the security executives we surveyed appreciate the potential for cyber to add value to the business growth agenda, the downside is that security teams are not yet consistently embedded with the digital transformation agenda. Part of the problem may be that security professionals often prefer to work with a fixed technology architecture, even though data flows and business processes are changing more rapidly than ever. A contributing factor may be the structure of cybersecurity teams within an organization, often straddling the line between IT and risk management, with reduced line of sight of the business strategy and growth agenda activities. Cybersecurity needs to match the agility of the digital organization, adapting to meet the fast-changing needs of stakeholders with the right mandate to enable digital transformation.



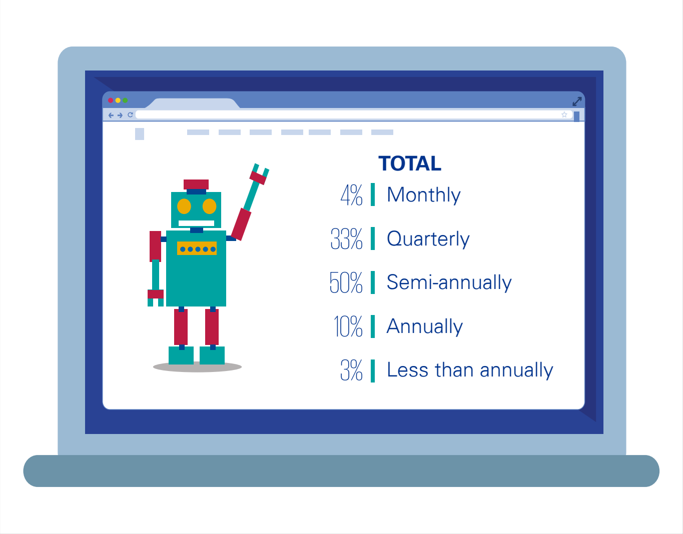
Source: Consumer Loss Barometer. Economics of trust. 2019.

Security challenges

Security on the business agenda

Cybersecurity is, unsurprisingly, gaining attention at the level of senior management; the vast majority of respondents provide a briefing to executives on at least a quarterly or semi-annual basis. This reinforces a finding in KPMG's 2018 Global CEO Outlook that the executives now rate cybersecurity threats the second-highest risk to their organization's future growth.

Sizeable minority say executives infrequently briefed on cybersecurity



Source: Consumer Loss Barometer. Economics of trust. 2019.

What is worrying is that, while all respondents noted that they are undertaking digital transformation activities, cybersecurity still only features at an executive level on an annual or less than annual basis for 24 percent of automotive and retail respondents.

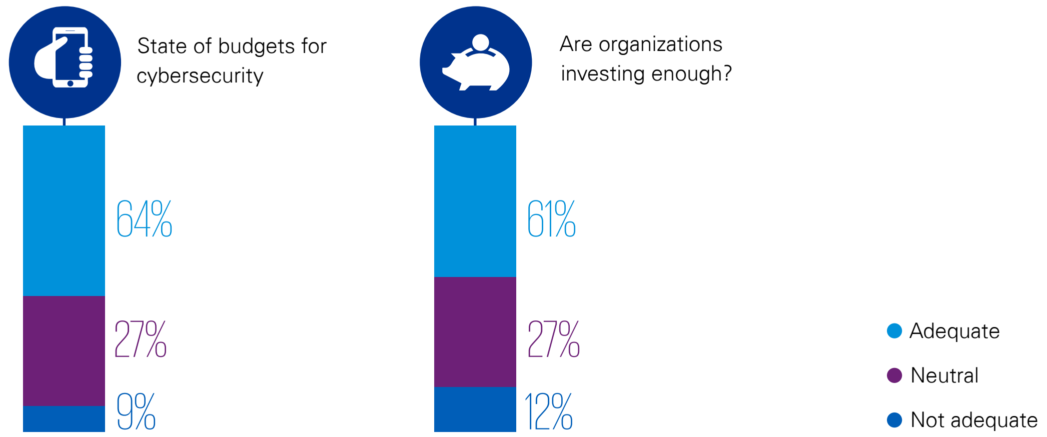
> "CEOs need to turn 'cyber concern' into 'cyber confidence'," *says* ***Dani Michaux****, Cyber Security Leader, KPMG in Malaysia.* "They must play an active part in cybersecurity discussions, while ensuring all the senior executives understand that cyber is a strategic priority. It's encouraging that 59 percent of CEOs see protecting customer data as a critical, personal responsibility. Now, they must translate those words into actions."

Are security professionals getting enough resources?

The majority of security professionals we surveyed agreed that data security budgets and investment levels are currently adequate to meet their objectives. However, at least a third do not feel that they receive adequate financial support from their organizations.

The next challenge for security teams is to demonstrate an acceptable return on investment. Through good governance, boards can better direct spending and ensure that it is optimized and linked efficiently and effectively to business and technology priorities.

Are there enough monetary resources for information security?

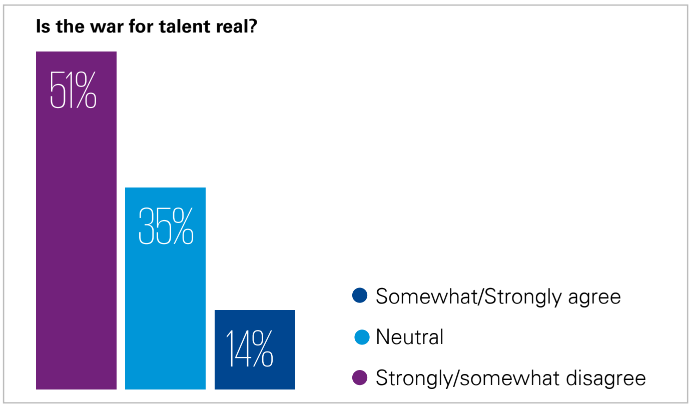


Source: Consumer Loss Barometer. Economics of trust. 2019.

Is the war for talent real?

Hiring and retaining the right talent is a critical part of an organization's security strategy, and is a challenge for the majority of the security executives we surveyed, with over half struggling to source talent to meet their needs. To meet this challenge, security executives will need to transform their own operations, and employ innovative methods to create fresh pools of talent, for example, by hiring people who have not received a traditional STEM education, or by upskilling their existing workforce to pivot the talent matrix.

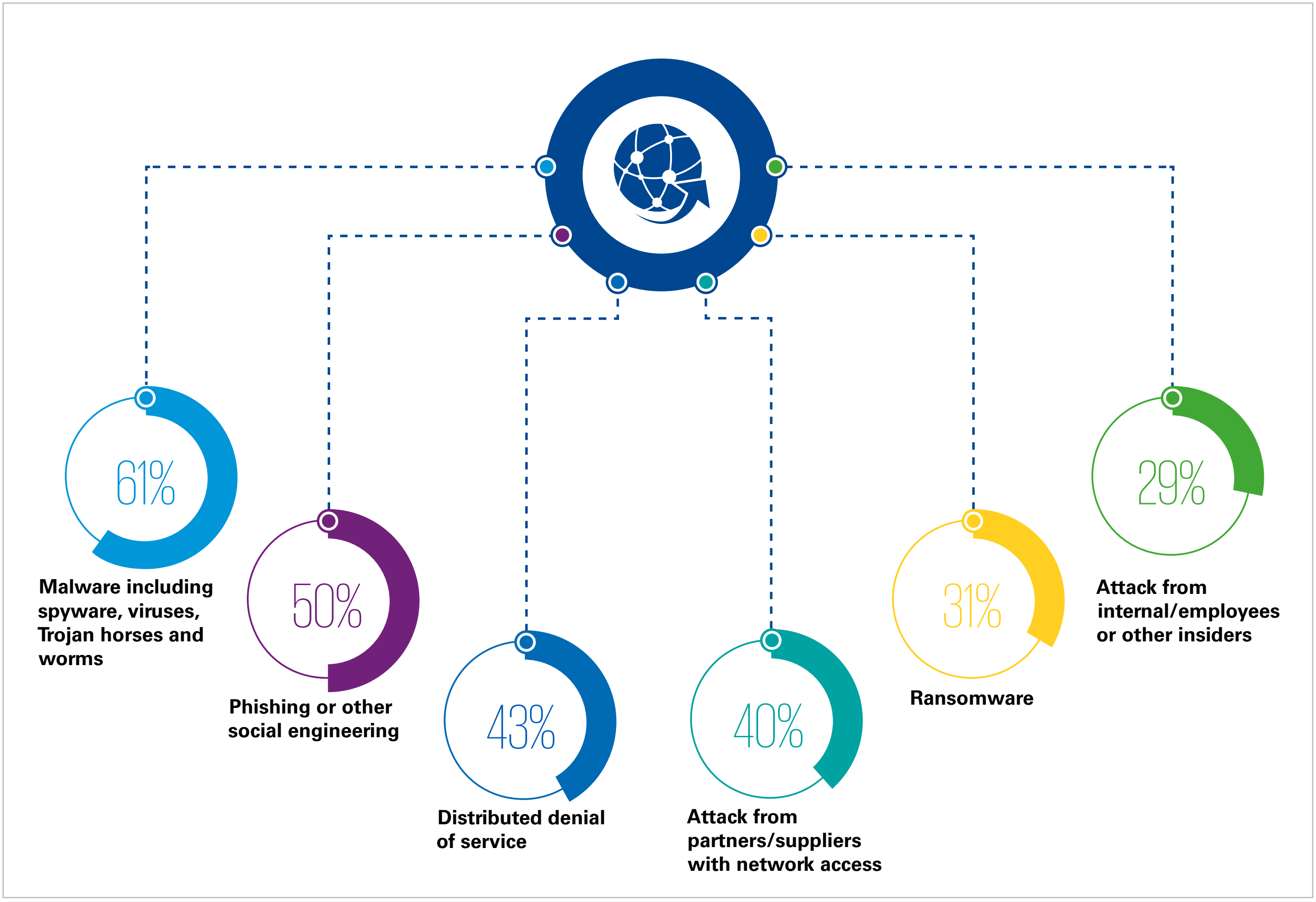
There is also scope to address the war for talent by redefining the business's labor model. Staff shortages can be addressed by increased automation, crowdsourcing and using skilled contractors.



Source: Consumer Loss Barometer. Economics of trust. 2019.

"Every organization needs to analyze what it is doing to attract and retain talent, and to ask itself the question: what activities are working and which ones aren't? There is never a ceasefire in the 'war for talent', only a better strategy and tactics," *says **Brian Geffert**, KPMG Global Chief Information Security Officer*. "In the future, the skills that will be required in the area of cyber are business and digital, as well as security, complemented by digital innovation."

What is concerning security professionals?



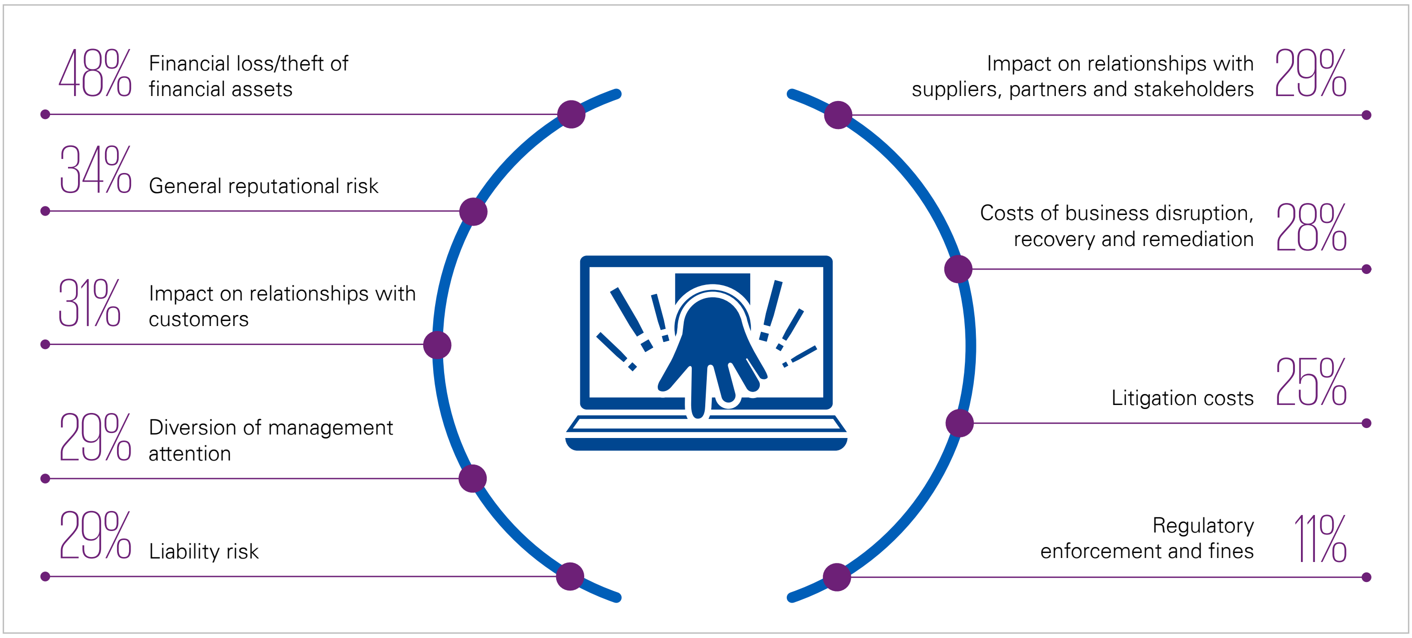
Source: Consumer Loss Barometer. Economics of trust. 2019.

According to the security executives we surveyed, malware is the top concern followed by phishing or social engineering. Distributed denial of service attacks is the third largest concern for organizations, with direct impacts on the company's ability to provide digital products and services. Despite multiple high profile, global incidents during 2018, ransomware such as NotPetya worried less than a third of respondees, with third-party access being of greater concern.

Security professionals should rightly be worried about attacks from partner and supplier networks, as cyberattackers shift their focus to target supply chains and the weak points in managed service providers, rather than larger, more mature companies that are harder to break into. E-commerce and digital channels are also becoming more of a target, as are cryptocurrencies.

> "Cybercriminals are looking for the biggest bang for the buck. As they seek to maximize their return on investment, they focus on what makes them the most money — and at the moment that is tricking firms into transferring funds through spearphishing and social engineering (so-called CEO frauds), extortion through ransomware, and attacks on the new world of cryptocurrencies." *says **David Ferbrache**, CTO, Cyber Security, KPMG in the UK.*

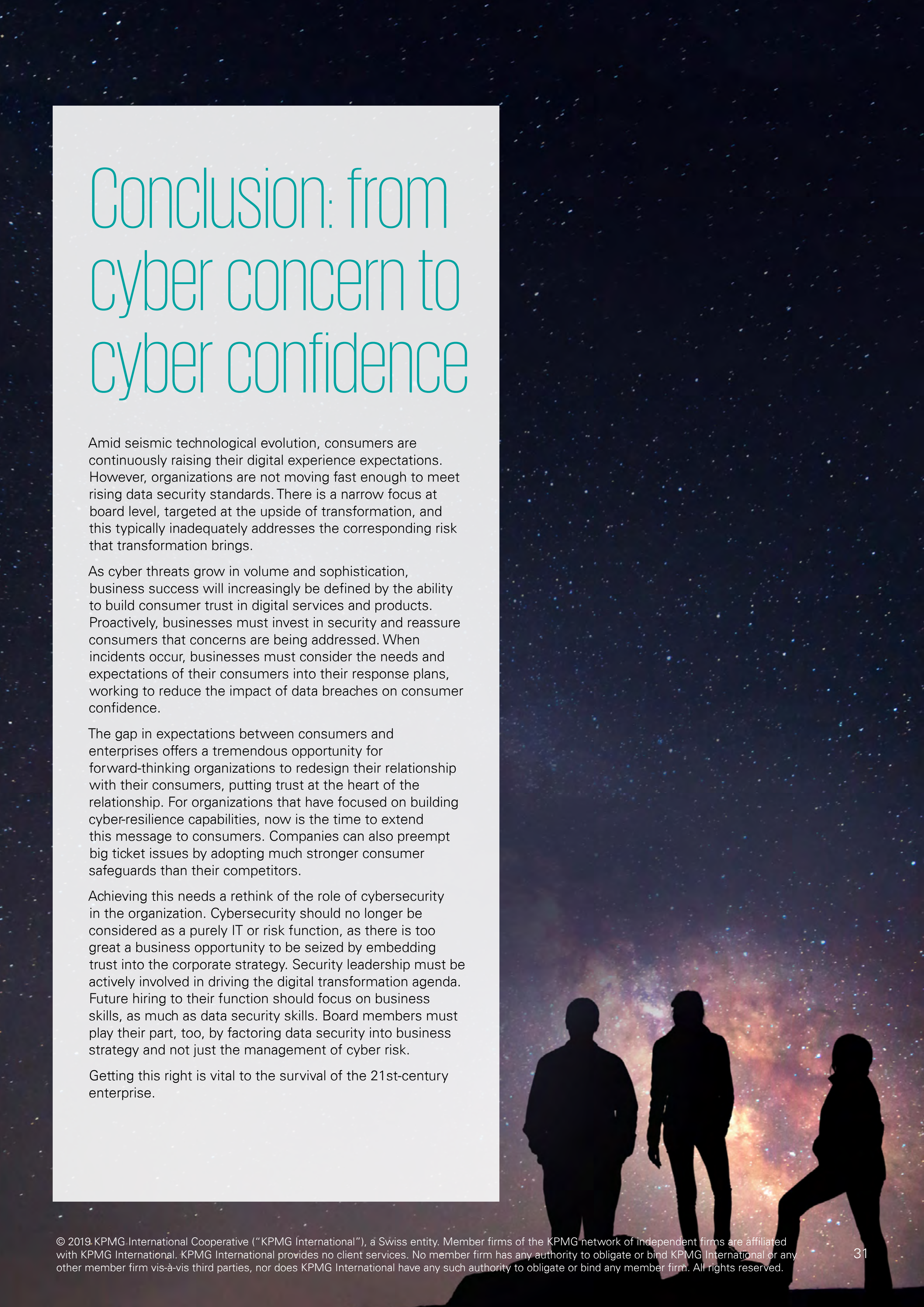
What concerns security leaders when a breach occurs?



Source: Consumer Loss Barometer. Economics of trust. 2019.

Surprisingly, despite the opportunity security executives see for cybersecurity to support customer engagement, less than a third of the survey respondents are concerned about the impact of a breach on the organization's relationship with customers. In the age of the customer, organizations need to prepare for an attack and determine a strategy for maintaining the trust of consumers throughout their response activities. In this way, consumers will not be forgotten about in the event of a breach.

> "New regulations, such as the GDPR, threaten to exact very heavy fines from organizations that break the rules as they relate to consumers. Trust is being demanded by both consumers and regulators, and companies will feel the pinch on their pockets from both sides when things go wrong," *says **John Hermans**, KPMG EMA Leader, Cyber Security.*



Conclusion: from cyber concern to cyber confidence

Amid seismic technological evolution, consumers are continuously raising their digital experience expectations. However, organizations are not moving fast enough to meet rising data security standards. There is a narrow focus at board level, targeted at the upside of transformation, and this typically inadequately addresses the corresponding risk that transformation brings.

As cyber threats grow in volume and sophistication, business success will increasingly be defined by the ability to build consumer trust in digital services and products. Proactively, businesses must invest in security and reassure consumers that concerns are being addressed. When incidents occur, businesses must consider the needs and expectations of their consumers into their response plans, working to reduce the impact of data breaches on consumer confidence.

The gap in expectations between consumers and enterprises offers a tremendous opportunity for forward-thinking organizations to redesign their relationship with their consumers, putting trust at the heart of the relationship. For organizations that have focused on building cyber-resilience capabilities, now is the time to extend this message to consumers. Companies can also preempt big ticket issues by adopting much stronger consumer safeguards than their competitors.

Achieving this needs a rethink of the role of cybersecurity in the organization. Cybersecurity should no longer be considered as a purely IT or risk function, as there is too great a business opportunity to be seized by embedding trust into the corporate strategy. Security leadership must be actively involved in driving the digital transformation agenda. Future hiring to their function should focus on business skills, as much as data security skills. Board members must play their part, too, by factoring data security into business strategy and not just the management of cyber risk.

Getting this right is vital to the survival of the 21st-century enterprise.

Contributors

Ivan Atanasov, Manager, Cyber Security, KPMG in the UK

Dieter Becker, Global Automotive Leader, KPMG International

Bia Bedri, Banking and Capital Markets Cyber Leader, KPMG in the UK

Greg Bell, Global Co-Leader, Cyber Security, KPMG International

Judd Caplain, Global Banking and Capital Markets Leader, KPMG International

David Ferbrache, CTO, Cyber Security, KPMG in the UKG in the UK.

Tim Fletcher, Director, Cyber Security, KPMG in the UK

Akhilesh Tuteja, Global Co-Leader, Cyber Security, KPMG International

Marko Vogel, Partner, Cyber Security, KPMG in Germany

John Hermans, EMA and Cyber Security Leader, KPMG in the Netherlands

Alex Holt, Global Chair, Media & Telecommunications, KPMG International

Willy Kruh, Global Chair, Consumer & Retail, KPMG International

Dani Michaux, Cyber Security Leader, KPMG in Malaysia

Thomas Nash, Manager, Cyber Security, KPMG in the UK

Gary Reader, KPMG Global Head of Clients and Markets, KPMG International

Jitendra Sharma Global Leader, Risk Consulting, KPMG International

Atul Gupta, Cyber Telco and Cyber Security Leader, KPMG in India

Paul Taylor, Partner, Cyber Security, KPMG in the UK

Contact us

Akhilesh Tuteja
Global Cyber Co-Leader
KPMG International
E: atuteja@kpmg.com

Greg Bell
Global Cyber Co-Leader
KPMG International
E: rgregbell@kpmg.com

The Americas

Tony Buffomante
Cyber Security Leader
KPMG in the US
E: abuffomante@kpmg.com

Francois Beaudoin
Cyber Security Leader
KPMG in Canada
E: fbeaudoin@kpmg.ca

Leandro Antonio
Americas Cyber Security Leader
KPMG in Brazil
E: lantonio@kpmg.com.br

Europe

Luca Boselli
Cyber Security Leader
KPMG in Italy
E: lboselli@kpmg.it

John Hermans
EMA Cyber Security Leader
KPMG in the Netherlands
E: hermans.john@kpmg.nl

Mika Laaksonen
Cyber Security Leader
KPMG in Finland
E: mika.laaksonen@kpmg.fi

Matthias Bossardt
Cyber Security Leader
KPMG in Switzerland
E: mbossardt@kpmg.com

Martin Tyley
Cyber Security Leader
KPMG in the UK
E: Martin.Tyley@kpmg.co.uk

Vincent Maret
Cyber Security Leader
KPMG in France
E: vmaret@kpmg.fr

Uwe Bernd-Striebeck
Cyber Security Leader
KPMG in Germany
E: uberndstriebeck@kpmg.com

Marc Martinez
Cyber Security Leader
KPMG in Spain
E: marcmartinez@kpmg.es

Asia Pacific

Matthew O'Keefe
ASPAC Cyber Security Leader
KPMG in Australia
E: mokeefe@kpmg.com.au

Gordon Archibald
Cyber Security Leader
KPMG in Australia
E: garchibald@kpmg.com.au

Daryl Pereira
Cyber Security Leader
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Henry Shek
Cyber Security Leader
KPMG in China
E: henry.shek@kpmg.com

Atsushi Taguchi
Cyber Security Leader
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Atul Gupta
Cyber Security Leader
KPMG in India
E: atulgupta@kpmg.com

Shaked Levy
Cyber Security Leader
KPMG in Israel
E: shakedlevy@KPMG.com

Methodology

The data published in this report is based on a survey of 1,802 security executives (or equivalent) in 24 markets, across 12 industries. All respondents were from companies with annual revenues between $100 million to $10 billion or more. The security executives (or equivalent) survey was translated in nine languages. Consumer data was based on a survey of 2,151 consumers in 24 markets. The sample included all age categories, with a higher percentage of Millennials and Gen Xers, as well diversified by gender. The consumer survey was translated in eight languages.

KPMG Cyber Security Services

KPMG Cyber Security 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 Security approach strategically aligns with clients' business priorities and compliance needs.

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.