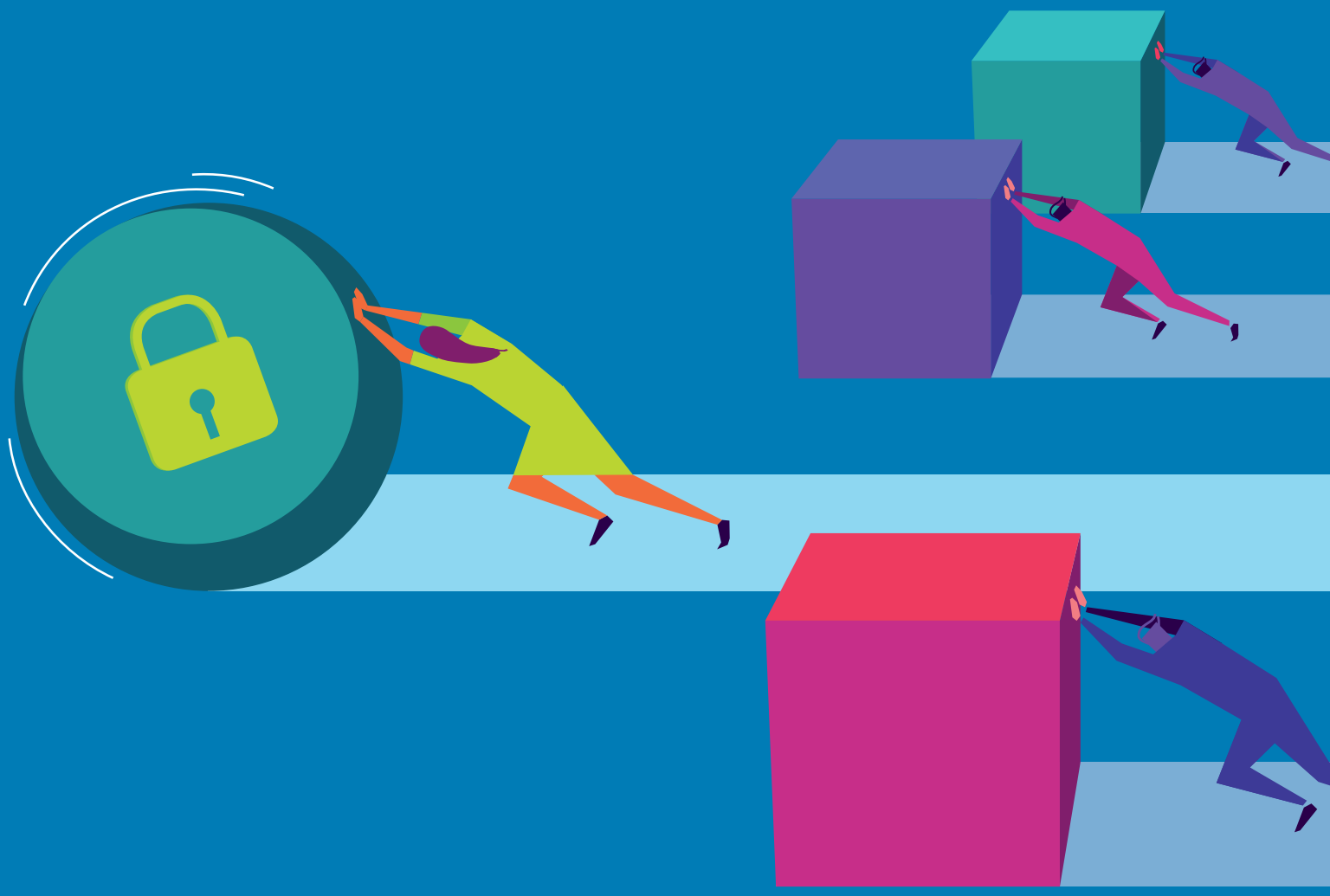
Capgemini
RESEARCH INSTITUTE

CYBERSECURITY

The new source of competitive advantage for retailers



Many companies have invested significant amounts of money in programs and technologies to improve cybersecurity—the protection of consumer data, enterprise information, and intellectual property. But while cybersecurity is often seen in terms of the cost of mitigation—or the ramifications of a breach—it is also a business driver and can be a source of competitive advantage in the retail sector.

We probed this issue in a global survey of over 6,000 consumers and 200 retail executives, as well as in interviews with experienced cybersecurity executives. The research methodology at the end of this report provides further details.

Our research reveals that customer satisfaction and spending can drastically be improved by cybersecurity and data protection assurance. Yet, very few retailers are leveraging this opportunity to gain competitive advantage. This report:

- Explores how cybersecurity and data protection is a business driver
- Assesses retailers' understanding of consumer expectations for cybersecurity and data privacy
- Quantifies the gains for a retailer with a robust cybersecurity and data protection system
- Provides recommendation on how retailers can leverage cybersecurity and data privacy to drive value and growth.

Cybersecurity is absolutely a business driver. A good cyber-defense system is an expectation from a customer standpoint and it should be from a business standpoint. A retailer must have the best available protection and security tactics today."

Retail executive
US department store

Cybersecurity and data protection is a business driver for retailers

Consumers prize cybersecurity when selecting retailers

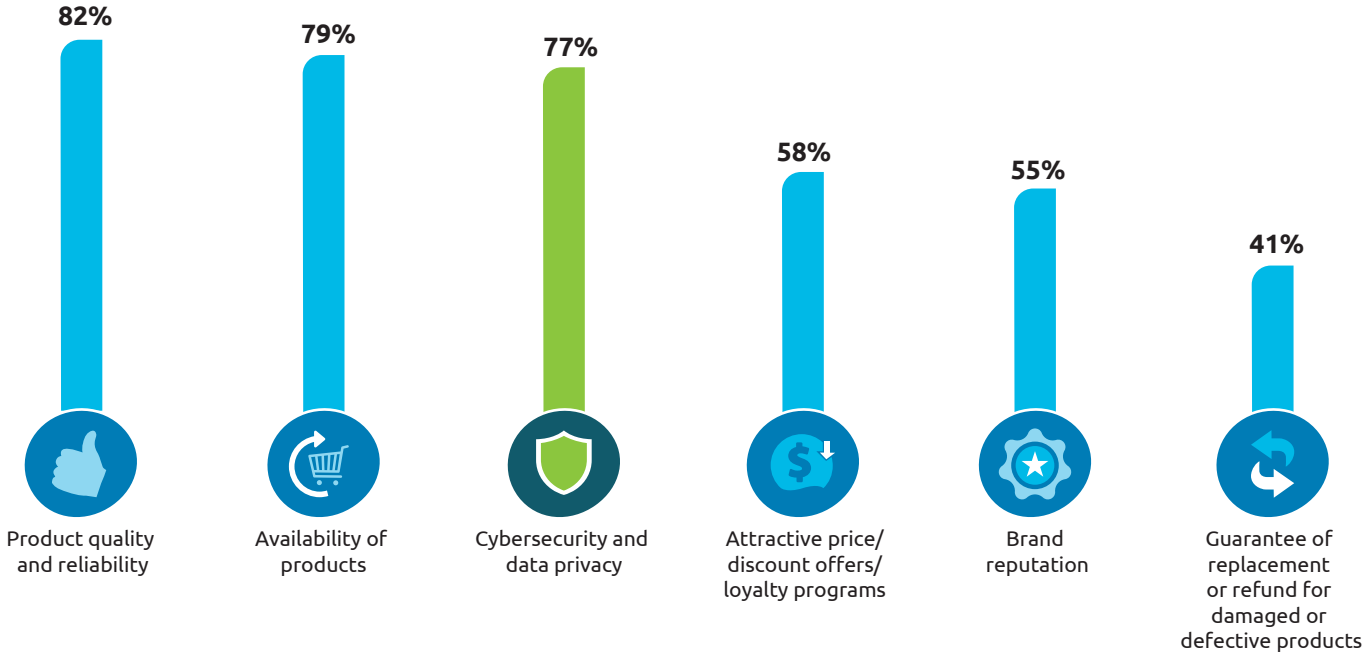
In our survey, we asked consumers to rank several criteria according to their importance when choosing a primary retailer (by that we mean the one they shop with most). Among criteria such as product quality, product availability, and discounts, we also asked about four factors related to cybersecurity and data privacy:

- Safety of in-store devices, such as kiosks
- Safety of websites and apps
- Safety of stored personal or financial data
- Transparency of the usage of stored personal or financial data.

We found that these factors are crucial when people are deciding on a retailer. For example, cybersecurity and data privacy outranked attributes such as discounts (see Figure 1).

Figure 1. Cybersecurity is an important factor when consumers' select retailers.

Percentage of consumers considering the following factors as one the top five criteria while selecting their primary retailer*



Consumers' ranking of cybersecurity and data privacy factors by country

Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

*Percentage denotes the share of consumers who selected each of the categories as one of the top five criteria for selecting their primary retailer.

Cybersecurity and data privacy through the eyes of the consumer

In this study, we analyzed consumers' perception of cybersecurity and data privacy along three dimensions:

Factors (how consumers judge retailers' cybersecurity and data privacy capabilities)

There are four factors that consumers think about when considering a retailer's cybersecurity and data privacy capabilities:

1. Safety of in-store devices (e.g., point-of-sale, self-service kiosks)
2. Safety of websites and apps (i.e., do they use advanced security techniques)
3. Safety of stored personal or financial data
4. Transparency of the usage of stored personal or financial data

Capabilities (the specific actions that consumers want retailers to take to improve their cybersecurity and data privacy)

Consumers want retailers to enhance cybersecurity and data privacy capabilities across the four factors using the following capabilities:

1. Encryption of stored data
2. Prompt for passwords while accessing accounts
3. Clear and transparent data privacy policy
4. Control on what customer data the retailer can store, and for how long
5. Use of advanced anti-malware tools at stores or servers for online shopping
6. Use of advanced data encryption in websites or apps
7. Use of PIN and chip cards instead of swipe and sign ones at stores
8. Dual identification—both with mobile device and using finger print or iris scan
9. Use of finger print or iris scan at stores
10. Fingerprint-based authentication on websites or apps

Assurances (the promises that consumers expect from retailers as the result of enhancements to cybersecurity and data privacy capabilities)

Consumers expect the following assurances because of enhanced cybersecurity and data privacy capabilities:

1. Retailer's websites and apps are safe to use
2. Retailers explain how they are going use their personal and financial information
3. The personal and financial data retailers collect will remain safe

Source: Capgemini Research Institute analysis.

2.5x

The increase in the share of satisfied customers that implementation of cybersecurity and data privacy capabilities can achieve

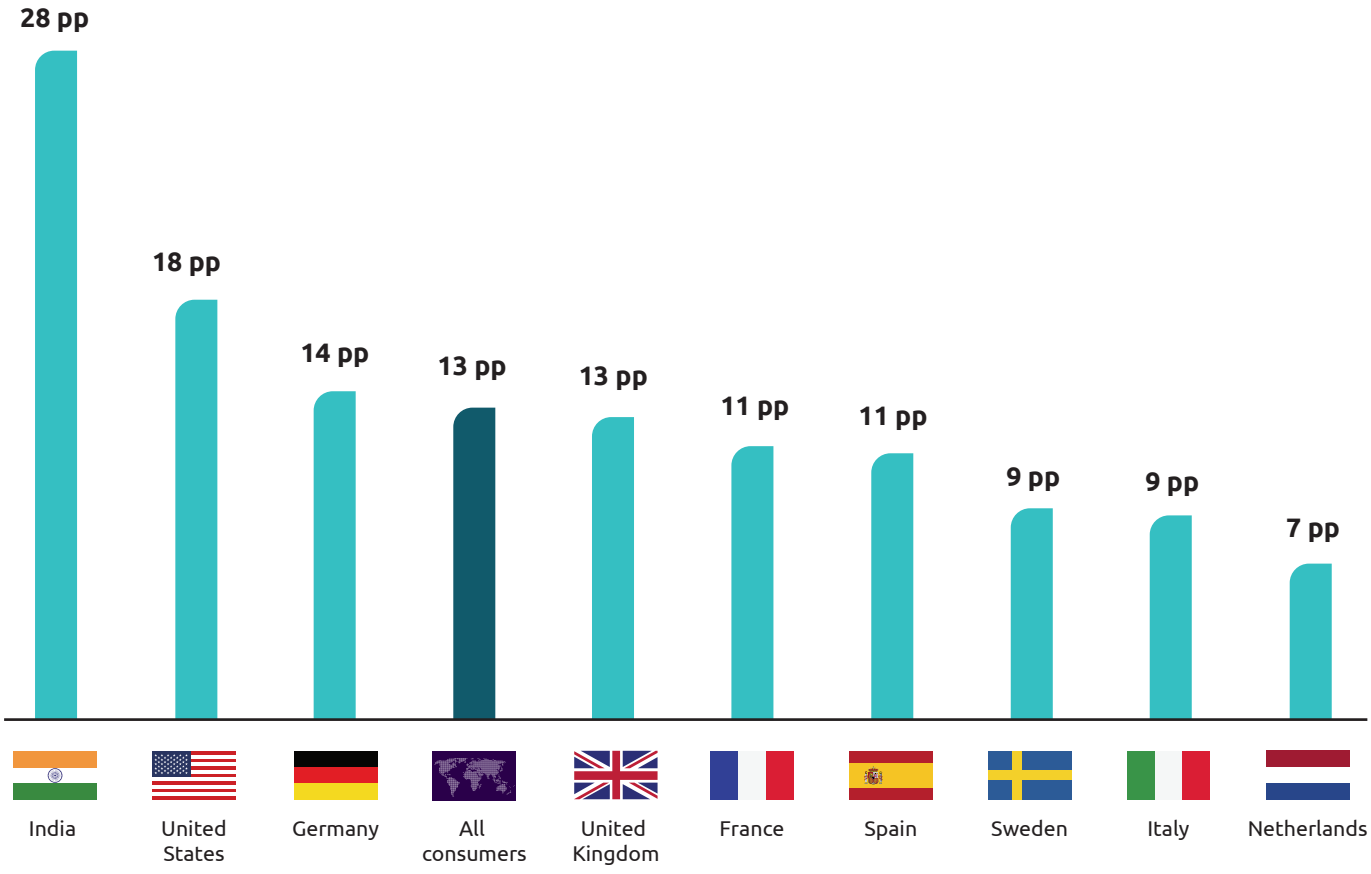
Cybersecurity and a transparent data policy drives customer satisfaction

To further test the importance of cybersecurity as a business driver, we measured a key metric for retailers—customer satisfaction. We asked consumers to rate how their satisfaction level would change if a retailer implemented a set of cybersecurity and data privacy capabilities (see Figure 3 for the details of these capabilities).

Globally, we found that the share of satisfied customers increased from 9% to 22% if consumers knew their primary retailer had implemented these capabilities. This is a 2.5x improvement in the share of satisfied customers. At a country level, as Figure 2 shows, Indian retailers have the greatest customer satisfaction potential. Retailers can secure a competitive edge over competitors by positioning themselves as safe custodians of customer data.

Figure 2. Share of satisfied customers improves considerably with implementation of security capabilities.

Average increase in the share of satisfied customers after implementation of cybersecurity and data privacy capabilities by country



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

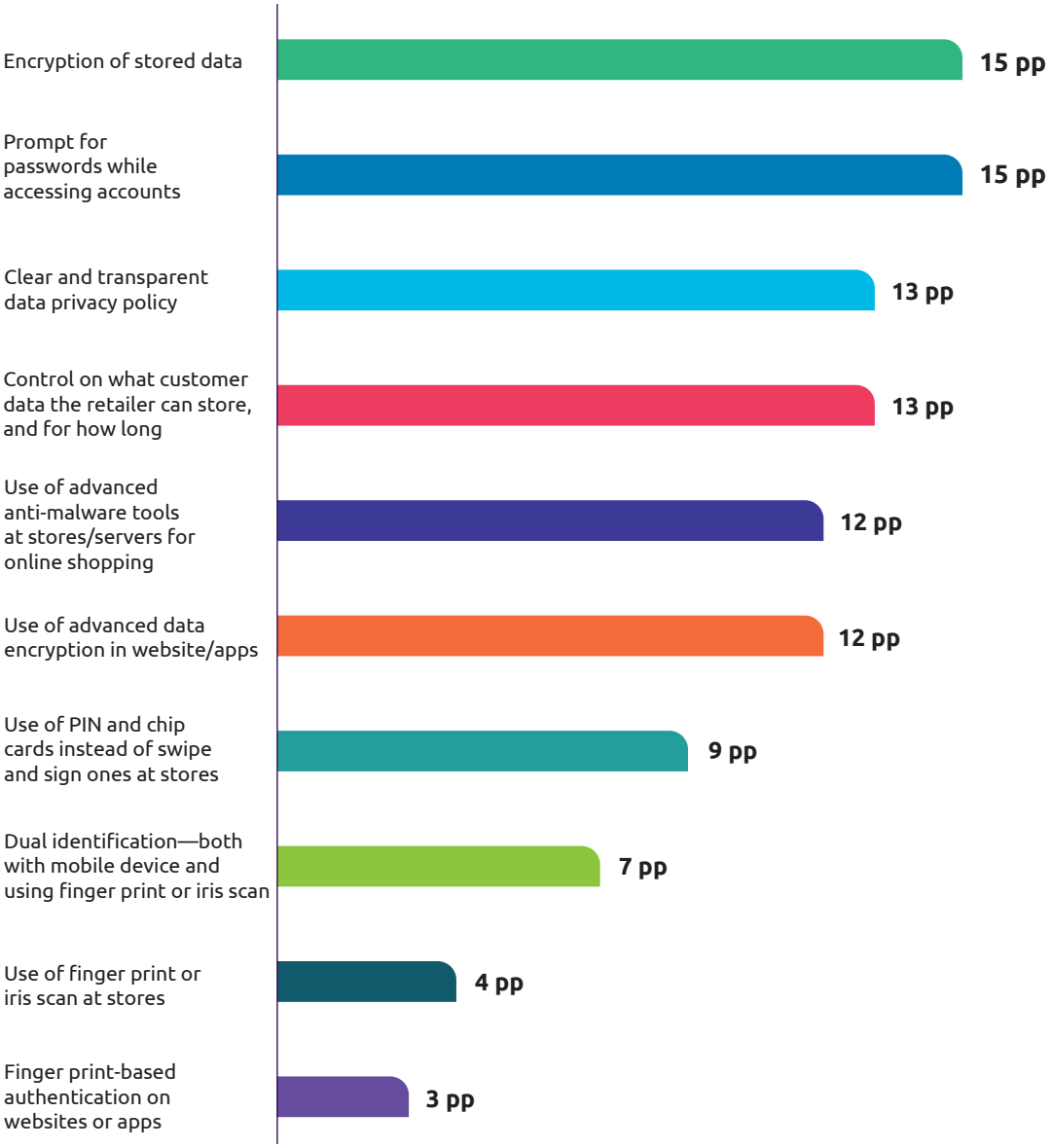
We also explored which specific cybersecurity and data privacy capabilities might be more important in driving customer satisfaction. The top capabilities are:

- Encryption of stored data (i.e., consumer's perception of a retailer's ability to protect their financial and personal information)
- Prompt for passwords while accessing accounts
- Transparent data privacy policy (i.e., policies that are easy to find and understand)
- Control over data retention.

These capabilities lead to the highest percentage point increase in share of satisfied customers (see Figure 3).

Figure 3. Encryption of stored data, password prompt, and a transparent data policy have greatest impact on customer satisfaction.

Percentage point increase in the share of satisfied customers if a retailer were to implement specific cybersecurity and data privacy capabilities



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

Consumers will increase online spending if they are assured of a retailer's cybersecurity practices and policies

We asked consumers how much they would increase online spending if a retailer were to take the following trust-building actions:

- Assure them that their financial and personal information was safe (e.g., by undertaking actions, such as proactive and periodic communication regarding security measures taken to protect consumers' data from the latest threats)
- Explain how their personal and financial information was going to be used
- Assure them that their websites and apps use the most advanced security techniques (e.g., 256-bit Secure Sockets Layer (SSL) encryption or Transport Layer Security (TLS).

As Figure 4 shows, approximately 40% of consumers would be willing to increase their online spend 20% or more if their primary retailer gave them these assurances which built their trust and competitors did not.

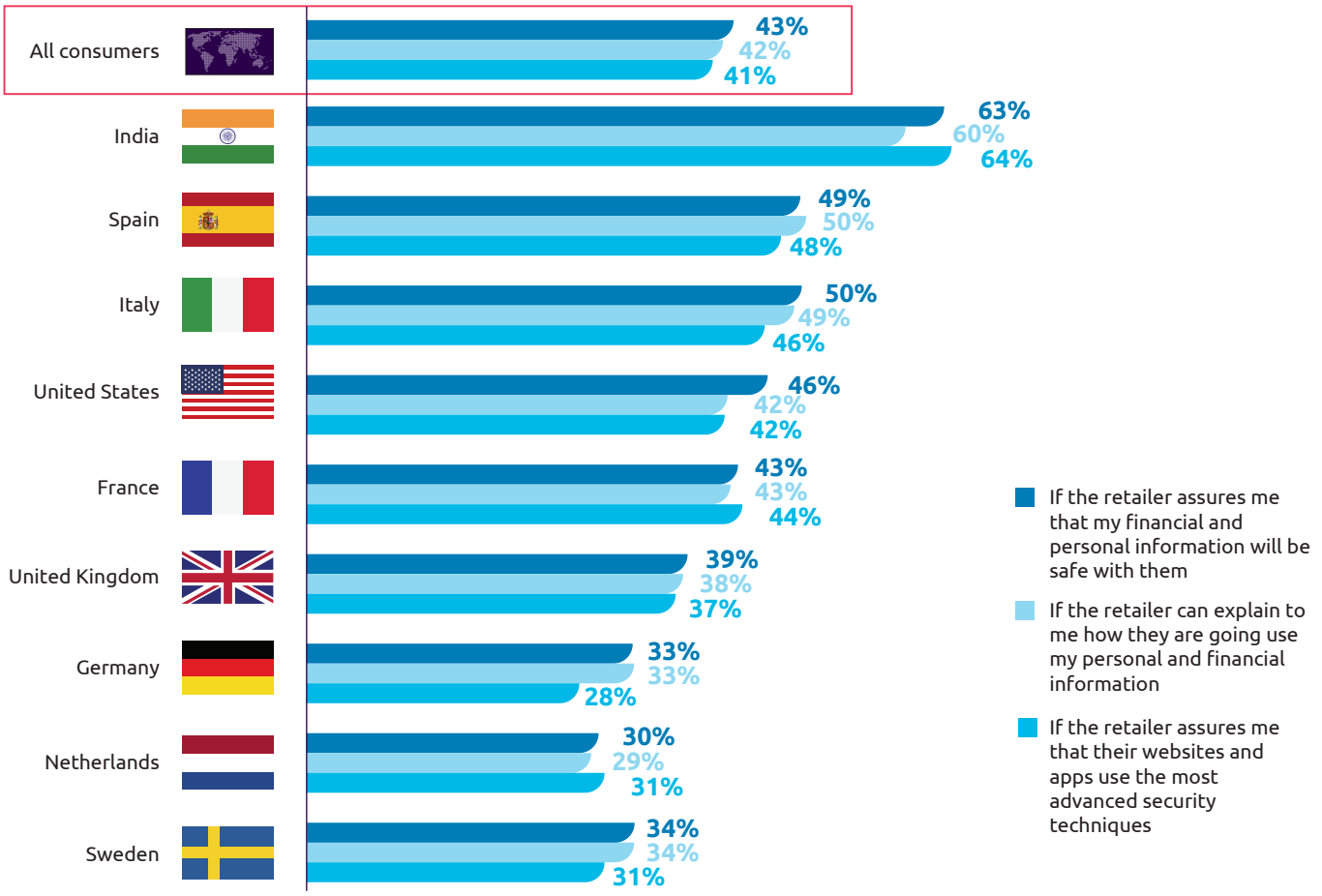
Of course, not all consumers are alike. Their sensitivity to cybersecurity and data privacy factors will vary, which will affect how likely they are to spend more online. We segmented consumers according to their sensitivity to these issues, ranging from those who were "not bothered" about these issues to those who we would characterize as "security and privacy obsessed" (see page 22 for more details on this segmentation). For example, only 20% of "least bothered" consumers are likely to increase their online spend 20% or more. However, this rises to 55% of the "security and privacy obsessed" cohort.

40%

Global consumers who will increase their online spend at least 20% if they receive certain cybersecurity and data privacy assurances from retailers

Figure 4. Around 40% of consumers are willing to increase their online spend by 20% if they receive assurances which builds their trust.

Percentage of consumers who are willing to increase their online spend by at least 20% if provided assurances, overall and by country



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

Cybersecurity can be a business driver for retail as long as the security platform is built considering the present as well as the future needs and the legacy systems of the organization."

Tyson Martin
Chief Information Security Officer,
the Orvis Company

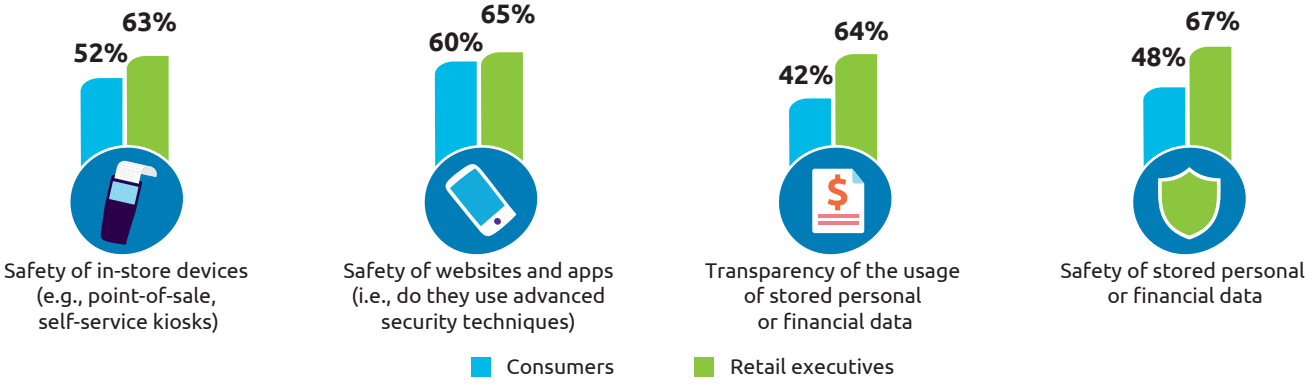
Retailers are missing an opportunity to use cybersecurity to drive growth

Executives are optimistic about their cybersecurity and data privacy capabilities, but consumers have a more downbeat view

We wanted to understand whether there were perception gaps between retailers and their customers. We asked consumers to rate their primary retailer on the four cybersecurity and data protection factors in Figure 5. We also asked retailers to rate how well they were doing. We found some significant disconnects, including transparency of use of personal and financial data.

Figure 5. Executives have a more optimistic view of their strengths than their consumers do.

Consumers who rate their primary retailer "outstanding" on cybersecurity and data privacy measures vs. retailer ratings*



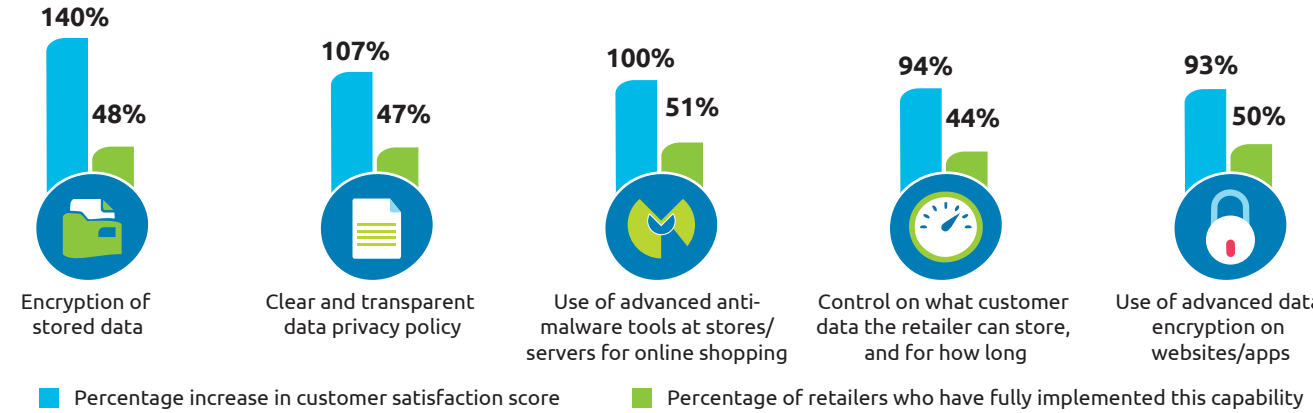
Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers; n=6,120 consumers.
*Percentage denotes consumer and retailer ratings of 6 or 7 on a scale of 1 to 7 where 1 = very poor and 7 = outstanding.

These disconnects are reinforced by four challenges:

1. **Most retailers do not focus on the cybersecurity and data privacy capabilities that can boost customer satisfaction.** Retailers do not appear to be focusing on the cybersecurity and data privacy capabilities that can drive customer satisfaction. There is a disconnect between the measures that retailers have implemented and the measures that consumers say will improve their satisfaction (see Figure 6). The same retailers tend to lack full implementation across all of the cybersecurity and data protection capabilities. The infographic on page 22 discusses this in greater detail.

Figure 6. More than half of the retailers have not fully implemented the capabilities that have the greatest impact on customer satisfaction.

Top five cybersecurity and data privacy capabilities driving customer satisfaction vs. their implemention status among retailers

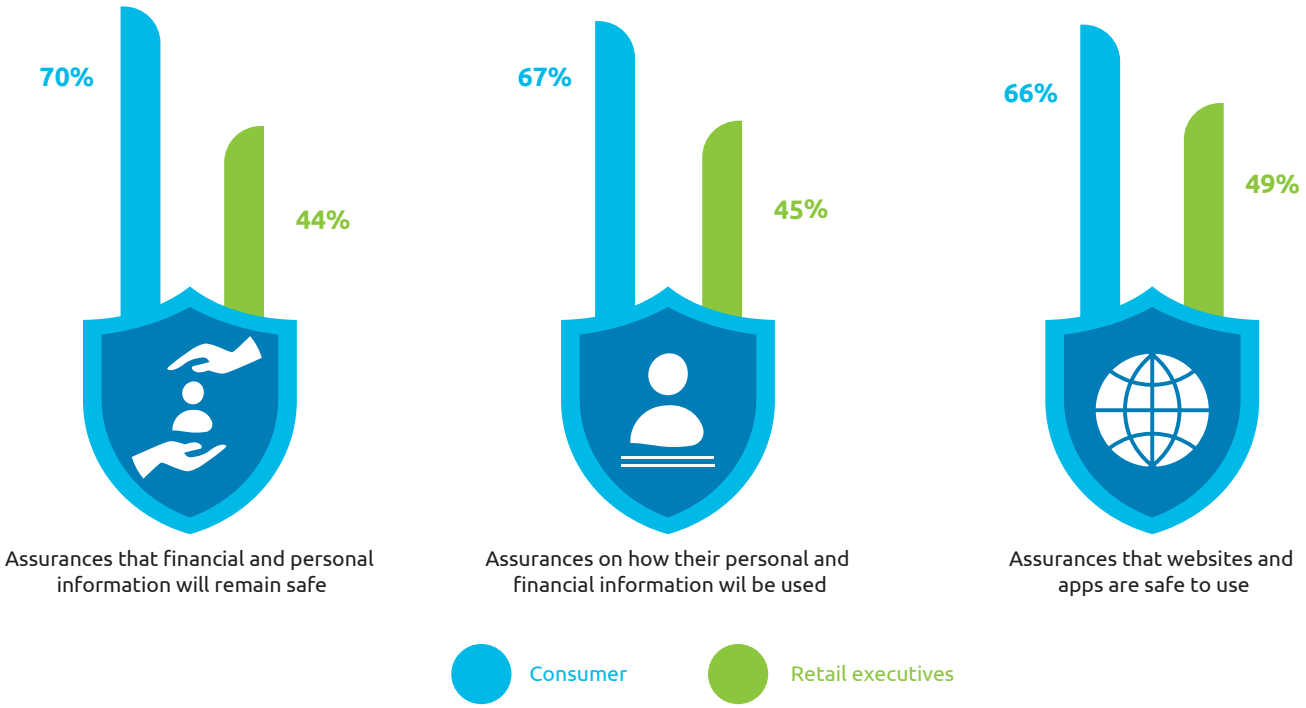


Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers, N=6,120 consumers.

2. **Consumers want more assurances from retailers than they are getting.** We asked consumers what would encourage them to purchase more online. Similarly, we asked retailers if their organization is taking or planning to take any of these actions to instill confidence in consumers to use their digital channels. Seventy percent of consumers want to be assured that their financial and personal information is safe, yet only 44% of retailers are taking this step (see Figure 7).

Figure 7. There is a disconnect between the assurances consumers want and what retailers are doing.

Consumers who would buy more online if assurances were made vs. actions retailers are taking



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers, N=6,120 consumers.

70%

Consumers who would buy more online if retailers assured them that their personal or financial information would remain safe

40%

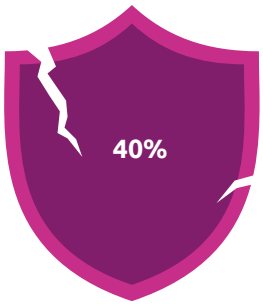
Percentage of retailers who experienced cybersecurity breaches over 2015–2017 that impacted consumer data

3. **Retailers appear reluctant to inform their customers of data breaches.** While data breaches experienced by retailers appear commonplace, consumers are not necessarily aware. Yet, consumers place great importance on being notified of a data breach. Fifty-seven percent of retailers said that they experienced a data breach over the past three years (2015-2017), and 40% of retailers said that customer financial or personal data was compromised. Yet only 21% of consumers said they had heard their primary retailer's name come up in relation to a security or data breach (see Figure 8).

Figure 8. Forty percent of retailers experienced a breach over the past three years and had customer data compromised, yet only 21% of consumers say they heard their primary retailer's name associated with a breach.

Percentage of retailers that experienced a data breach and had customer data compromised

Retailers who experienced a data breach over 2015 to 2017



Retailers who experienced a data breach over 2015 to 2017 and had customer personal or financial data data compromised

Percentage of consumers who have heard their primary retailer's name associated with a breach

Yes, my primary retailer's name has been mentioned with a security or data breach

No, my primary retailer's name has not been mentioned with a security or data breach

Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers; N=6,120 consumers.

The number of data breaches continues to increase. The UK's Information Commissioner's Office (ICO) recently revealed that the number of retail firms reporting data breaches doubled in just one year from 2016 to 2017.[1]

However, when the General Data Protection Regulation (GDPR) is implemented, the disconnect between incidents and customer awareness will change significantly. The GDPR requires all organizations to report certain personal data breaches to the relevant supervisory authority. It also requires individuals to be notified—within 72 hours of the organization becoming aware of the breach—if the breach is likely to adversely affect their data.[2]

4. **Few retailers inform their consumers of a breach before the media.** Most consumers (66%) say that they would stop or drastically reduce transactions if they learned from the media that their primary retailer suffered a data breach, regardless of whether consumers' data had been compromised during the breach. However, only 31% of retailers say that they reached out to their customers to inform them of a data breach in advance of the media (see Figure 9).

Figure 9. Few retailers reach out to their customers before the news is out in the media.

Percentage of consumers who would stop or reduce transactions vs. percentage of retailers who have reached their customers

Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers; N=6,120 consumers.

For the Orvis Company's Tyson Martin, customer data is a significant vulnerability for the retail sector.

"I think we (as retailers) have a decent-sized target on our backs," he says. "It's about access and visibility. People can see our products and services and the exchange of money for those goods, and they understand the scale right away. And coupled with the collection, storage and processing of our customer data … this is a large risk and our biggest vulnerability."

Enhanced cybersecurity and data protection could drive a revenue uplift of around 5%

A robust cybersecurity system and transparent data privacy policy can drive significant value

Getting cybersecurity and data policies right builds trust and drives customer satisfaction. As we saw in our previous study on loyalty, emotions are the main driver of consumer engagement and long-term loyalty. Our research found that honesty and trust were the top two emotions with the greatest influence. Security and whether a consumer "feels secure" with a brand is also a strong influence.[3]

Our current research finds that enhanced cybersecurity and data protection builds consumer trust for online transactions. Steve Woods, the deputy commissioner of policy at the ICO—the UK national data protection authority—recently expressed a similar opinion while speaking on GDPR. *"There is a major opportunity and competitive advantage for those who can demonstrate that they get data protection right,"* he said. *"Through changing their data handling culture, organizations can derive new value from customer relationships."*[4]

Some organizations have started to embrace this idea. Apple's recent launch of a privacy website shows how it wants to differentiate itself through care of customer data.[5] Apple uses clear and simple explanations to describe its privacy policies that consumers can easily understand.[6] Google also offers a consumer-friendly security website that clearly articulates what it's doing to keep customer data protected.[7] Similarly, Microsoft uses "just-in-time" notices—a practice advocated by the ICO—to clarify any customer concern at the time of providing data. For example, when a customer creates an account and inputs their birthdate, a pop-up window will appear that details why this information is being requested and how it will be used.[8]

To estimate the top-line value of making improvements to cybersecurity and data protection, we built a model for an average hypothetical US-based apparel and footwear retailer with a customer base of one million. Building on the results of our survey data, we found that this retailer could drive an additional 5.4% in annual revenue by adopting certain measures to improve consumer trust (see Figure 10). For example:

- Assuring customers that their websites and apps use the most advanced security techniques
- Assuring customers that their personal and financial information will remain safe.

The increase in online spend will come from curtailing spend on other retailers' online channels in which consumers have less trust.

Figure 10. Enhancing cybersecurity and data privacy could drive 5.4% uplift in retailers' annual revenue.

A. Average annual spending per customer *(from BLS data)**	US $1,803
B. Share of online spending *(from survey data analysis)*	24.12%
C. Average annual online spending per customer *(A x B)*	$434.88
D. Total customer base	1 million
E. Retailers annual revenue *(A x D)*	$1.80 billion
F. US consumers' willingness to increase online spending if cybersecurity and data privacy factors are enhanced[10] *(from survey data analysis)*	22.30%
G. Potential increase in annual revenue due to increased online sales *(C x D x F)*	$96.98 million
H. Estimated positive impact on top-line revenue *(G / E)*	5.38%

Source: Capgemini Research Institute analysis; Bureau of Labor Statistics.

*2016 average expenditure per consumer unit for apparel and services in the US; consumer unit defined as families, single persons living alone or sharing a household with others but who are inancially independent, or two or more persons living together who share expenses.

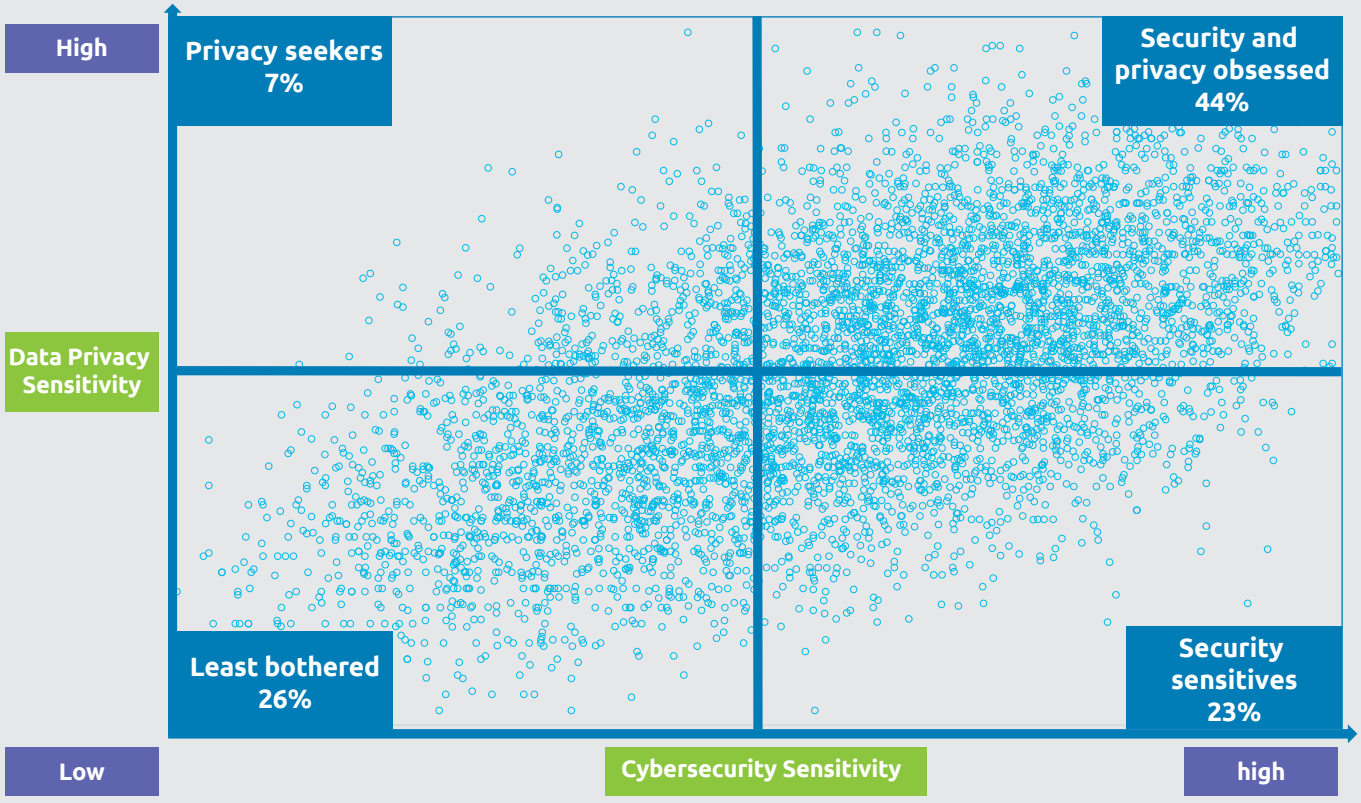
How sensitive are consumers to cybersecurity and data privacy?

We wanted to understand the importance of cybersecurity to consumers at a deeper level. We therefore assessed the response of every consumer about their preferences or expected behavior around cybersecurity and data privacy.
We classified consumers into four categories:

- Least bothered (26%)—those who scored low on both data privacy and cybersecurity dimensions
- Security sensitives (23%)—those who scored low on data privacy, but scored high on cybersecurity
- Privacy seekers (7%)—those who scored high on data privacy, but low on cybersecurity
- Security and privacy obsessed (44%)—those who scored high on both the dimensions.

We found that nearly half of consumers have high sensitivity for both cybersecurity and data privacy and nearly 70% are sensitive to security-related incidents. Furthermore, three-fourths of consumers are sensitive to at least one dimension (see Figure 11).

Figure 11. Nearly 50% of consumers have high sensitivity to cybersecurity and data privacy.



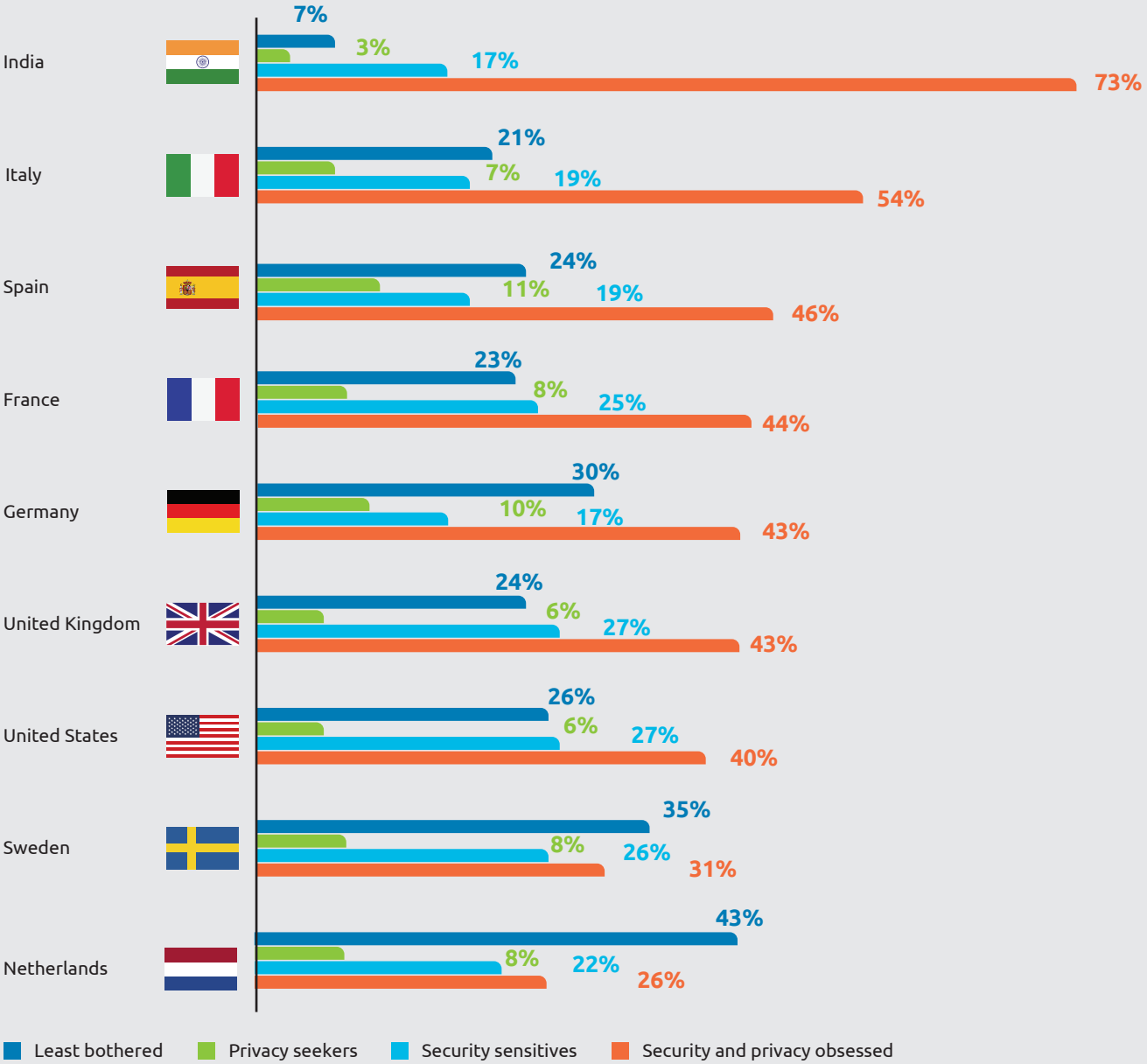
Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

We also looked at consumer sensitivity by country of residence. The lowest and highest percent of consumers within each segment include:

- 7% of consumers in India are least bothered vs. 43% in the Netherlands
- 3% of consumers in India are privacy seekers vs. 11% in Spain
- 17% of consumers in Germany and in India are security sensitives vs. 27% each in the UK and the US
- 26% of consumers in the Netherlands are security and privacy obsessed vs. 73% in India

Figure 12. Consumer sensitivity to cybersecurity and data privacy varies by country.

Percentage of consumers in each country by segment



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

Over 50% of the security-and-privacy-obsessed segment (22% of our overall sample) would increase their online spend if the retailer assured them that their personal and financial data would be safe or of the retailer explained how their personal data would be used (see Figure 13).

Figure 13. Over 50% of security and privacy-obsessed consumers are willing to increase their online spend at their primary retailer curtailing spend on other retailers if their primary retailer makes certain assurances.

Percentage of consumers who are willing to increase their online spend by at least 20% if provided assurances by segment

Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers.

How retailers can leverage cybersecurity and data privacy to drive value and growth

Without a doubt, security and information should be the number one thing every single retail company is looking at and focused on right now in this world. But it's not."

IT Director at a health-related retail company

Cybersecurity and data privacy can be a source of competitive advantage for retailers. There are several actions that retailers can take to seize this opportunity. At a high level, they comprise three steps:

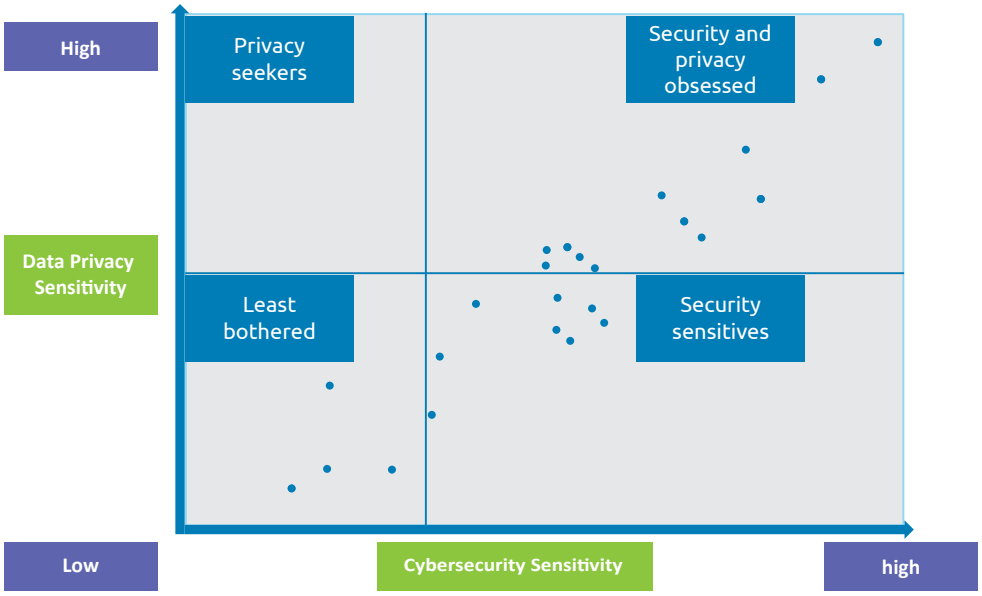
Understand your customers' cybersecurity and data privacy expectations and ensure the required features are fully implemented

The journey begins by understanding your customers' expectations and their sensitivity to cybersecurity and data privacy. As we saw earlier, most retailers have not implemented the cybersecurity factors that have most positive impact on customer satisfaction (refer to Figure 6). There is a gap between what consumers prize and what retailers deliver.

Consumer sensitivity to these issues will vary by retailer. As we outlined previously, we segmented consumers into groups that ranged from those who were obsessed with security to those who were largely "not bothered." Figure 14 shows these four groups mapped against 24 key primary retailers. Each retailer has different profiles, but "security sensitives" and "security and privacy obsessed" are most common (see Figure 14).

Figure 14. Most of the retailers' customers are in the security sensitives or security and privacy-obsessed segments.

Average sensitivity of customers of different retailers



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=6,120 consumers (N=5,907 for the company data).

Retailers can better understand this gap between what customers want and what retailers deliver by taking a number of actions; for example, educating customers on the "what, how, and why" of cybersecurity and data protection and asking them for their feedback on the measures that the organization has taken. Retailers can also build a picture of customers' sentiment on cybersecurity and data privacy on social media.

Get your cyber-defense system one step ahead of hackers

Given that news of a data breach will destroy customer trust, retailers need to keep cyber-defense systems ahead of the curve. The following actions are key:

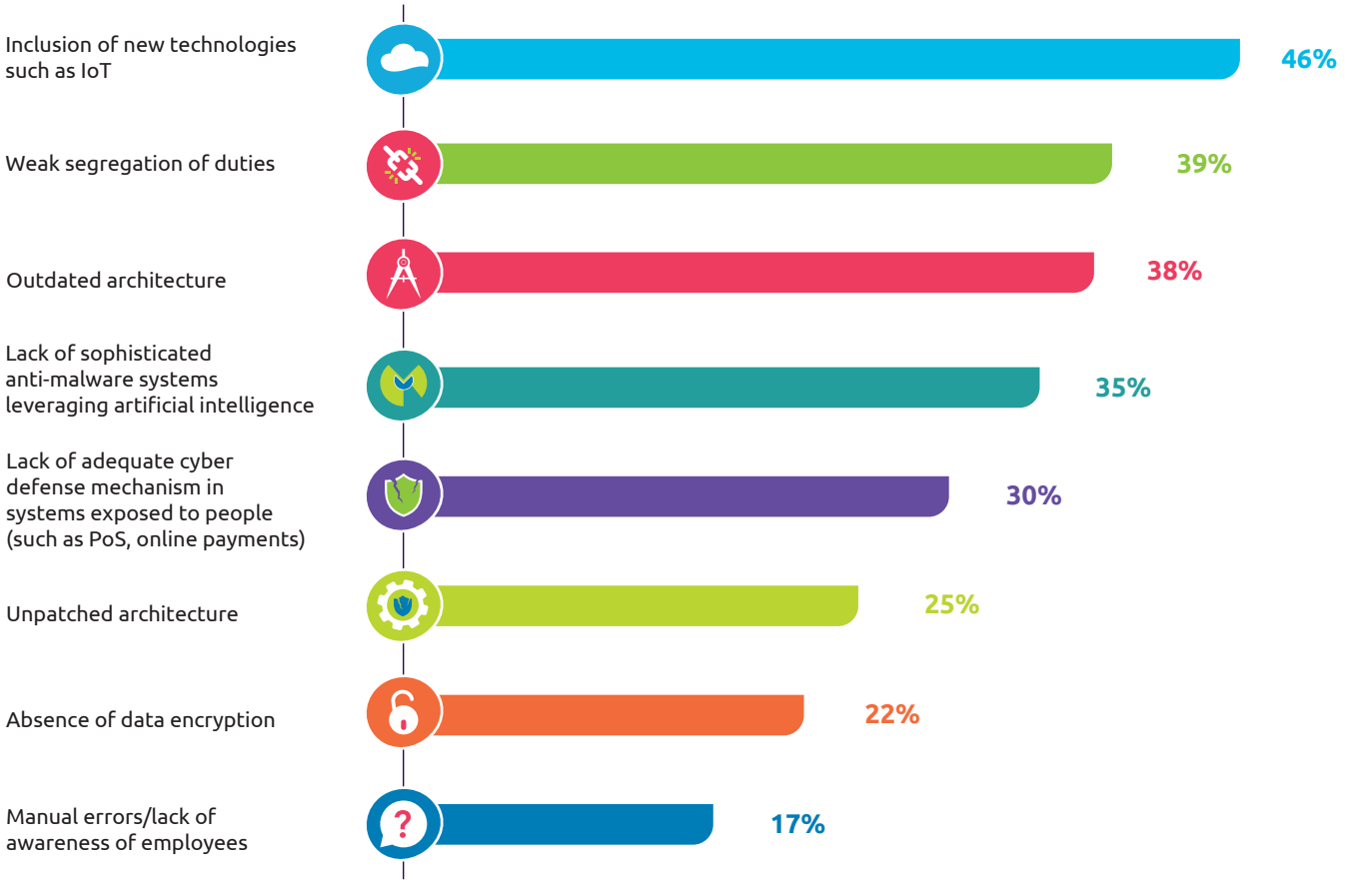
1. Understand your organization's vulnerabilities and plug the gaps
2. Identify the biggest threats in terms of likelihood and impact and adopt best practices to detect them
3. Involve top management to ensure adequate investment in security
4. Develop an incident-response plan to prevent customer churn.

1. Understand your organization's vulnerabilities and plug the gaps

Our survey reveals the top three vulnerabilities that were exploited by hackers during breaches at retailers in the last three years. These were: the inclusion of new technologies such as the Internet of Things, weak segregation of duties, and outdated architecture (see Figure 15).

Figure 15. Inclusion of new technologies, weak segregation of duties, and outdated architectures are the top vulnerabilities of retailers that lead to breaches.

Vulnerabilities that lead to cybersecurity breaches at retailers



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

Less than 50%

Retailers who perform application or infrastructure security audits daily or weekly

But, we found that retailers are not taking steps to shore up their defenses:

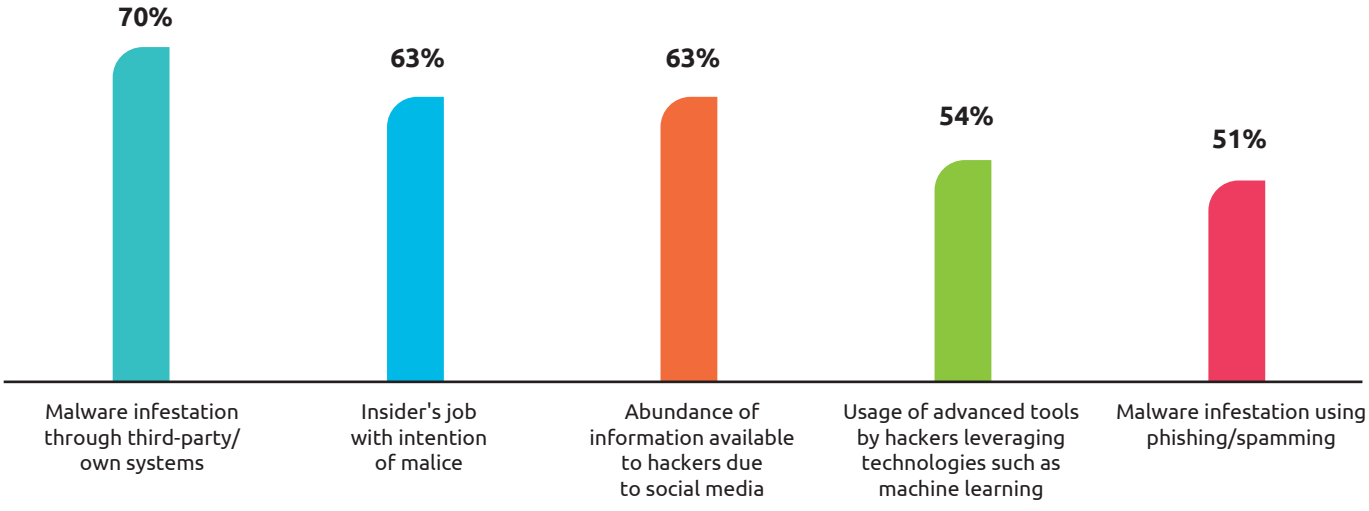
- Less than half perform daily or weekly audits into areas such as application security. This means a breach or a vulnerability might go undetected for seven days or more.
- Many are not running regular cybersecurity awareness programs. For example, only 43% run awareness programs for employees every two to four months. Given the high rate of employee turnover in retail, and part-time nature of many in-store jobs, running awareness programs frequently to educate employees is key to managing risks such as weak segregation of duties and manual errors. But Feizal Mussa, Information Security Manager at One Stop Stores, believes this is a neglected area. *"Retailers often don't have the right awareness programs for cybersecurity and humans are the weakest link when it comes to security,"* he says. A retail executive at a US-based department store also points out that employee churn in the sector makes regular programs essential, saying: *"In retail, you have this enormous workforce that unfortunately turns very quickly, so education and awareness needs to happen more often than in other sectors."*
- If we take common cyber-defense mechanisms¬¬—such as firewalls, identity access management, network segmentation, etc.—we find that many retailers are yet to fully implement (i.e., move beyond pilot or partial roll-out). For example, only 45% have fully implemented firewalls. Feizal Mussa believes this to be a glaring problem. *"Legacy systems are prevalent in retail,"* he says. *"Some systems are so basic that they do not even allow password complexity. A lot of retail environments are still running Windows 2003. Therefore, the legacy infrastructure is not able to support new-age technologies like AI."* The security officer at a high-end men's apparel retailer believes out-of-date infrastructure is a significant issue. *"Outdated infrastructure is a key vulnerability in the retail sector,"* she explains. *"I do see retailers making investments to update infrastructure. They are also expanding their use of emerging technologies, such as AI and the IoT. However, many retailers do not comprehend the risks that are involved in using those technologies."*

2. Identify the biggest threats in terms of likelihood and impact and adopt best practices to detect them

As well as understanding the vulnerabilities in your systems, you need to understand the threats that can exploit those vulnerabilities. In our survey, retail executives reported that malware infestation, "insider jobs" and the abundance of information available to hackers on social media are the greatest causes of cybersecurity breaches in the last three years (see Figure 16).

Figure 16. Malware infestation through third-parties, "insider jobs," and information available on social media are the biggest threats.

Threats that led to cybersecurity breaches at retailers



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

Our study reveals that many retailers are yet to implement common best practices to combat these threats. For example, using sandboxing and whitelisting techniques to analyze patterns, network traffic, intrusion detection systems, and deception techniques (e.g., intruder traps). While 56% say they have rolled out intrusion detection for example, this leaves a significant number of firms that do not.

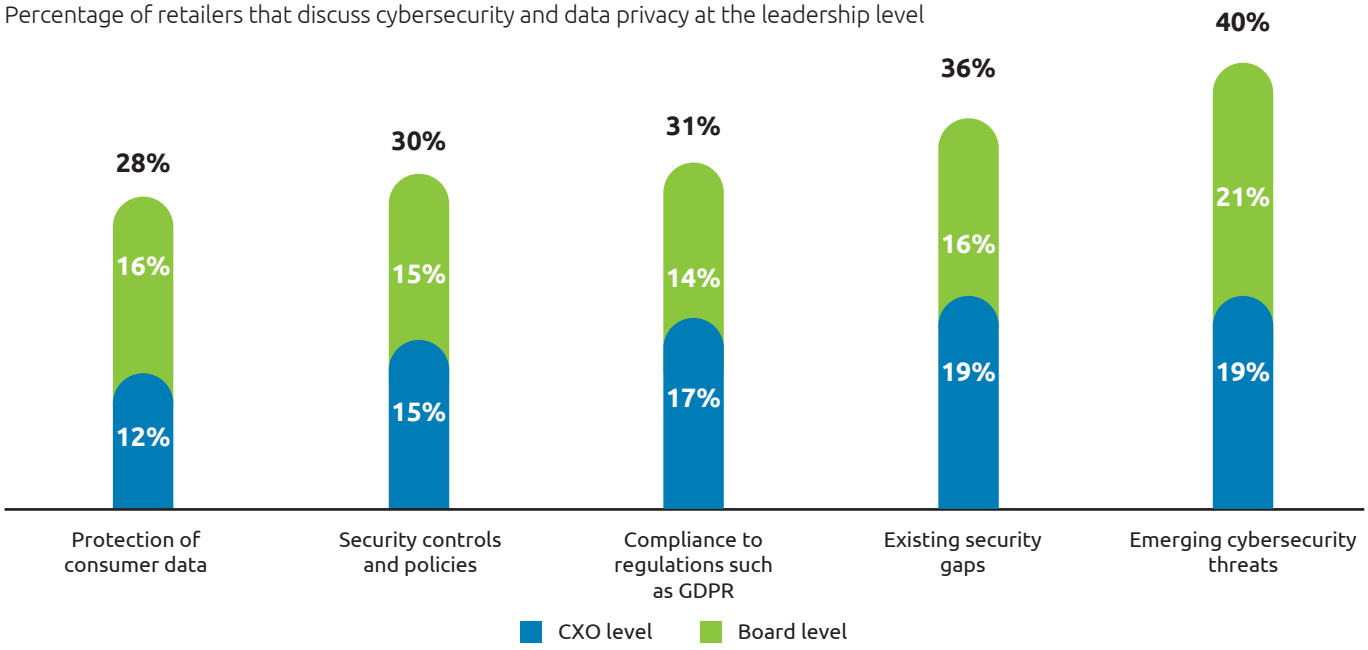
3. Involve top management to ensure adequate investment in security

The planned cybersecurity budget for the majority of retailers in our survey (57%) is less than $50 million for the next three years.[9] This might not be enough to build a robust cybersecurity system, given these factors:

- The magnitude of customer accounts (1.2 million accounts, on average)
- Volume of transactions (13,535 per hour, on average)
- The fact that many best practices for threat detection and vulnerability reinforcement are yet to be implemented. Feizal Mussa believes that retail has a culture of under-investment compared to other sectors. *"Financial services is highly regulated and therefore institutions have the money to invest in security. But, within retail, I often hear the phrase, 'more bang for my buck.' Retail is all about making sure whatever money we put into anything, we get the most value and the best return. Generally, this leads us to underinvest in technology and security."*

The potential for under-investment may stem from the fact that top leadership are less involved in the cybersecurity agenda, as Figure 17 shows.

Figure 17. Few retailers monitor cybersecurity at the executive leadership level.



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

Speaking on the need for buy-in at all levels, Tyson Martin says:
Everyone needs to understand the connection between their decisions and actions, at board and C-level, vice-presidents and directors, and managers and staff members. For example, understanding how opening an unknown email attachment—or bringing in a device that is not connected to the internet in a secure way—can create risk."

4. Develop an incident-response plan to prevent customer churn

Our analysis shows that a solid cyber-defense system, complemented with a well-planned incident response plan, can restrict customer churn by up to 86%.[10] As part of a well-planned incident response plan, organizations need to consider the following steps:

- Report the breach to customers and relevant authorities
- Implement a solution to fix the exploited vulnerability and minimize the damage
- Identify the cause
- Assess the damage
- Come up with concrete steps to prevent similar breaches in the future.

However, our study shows that retailers miss out on quite a few key steps (see Figure 18). Most effort is concentrated on implementing persistent threat detection and data leak prevention. However, other important tactics appear to be less of a priority, including:

- Recruiting cyber-forensic experts to analyze the root cause
- Forming or strengthening incident-response teams to assess the impact
- Communicating with customers and authorities.

A key step for retailers is to have a robust plan, as a retail executive from a US-based department store says:

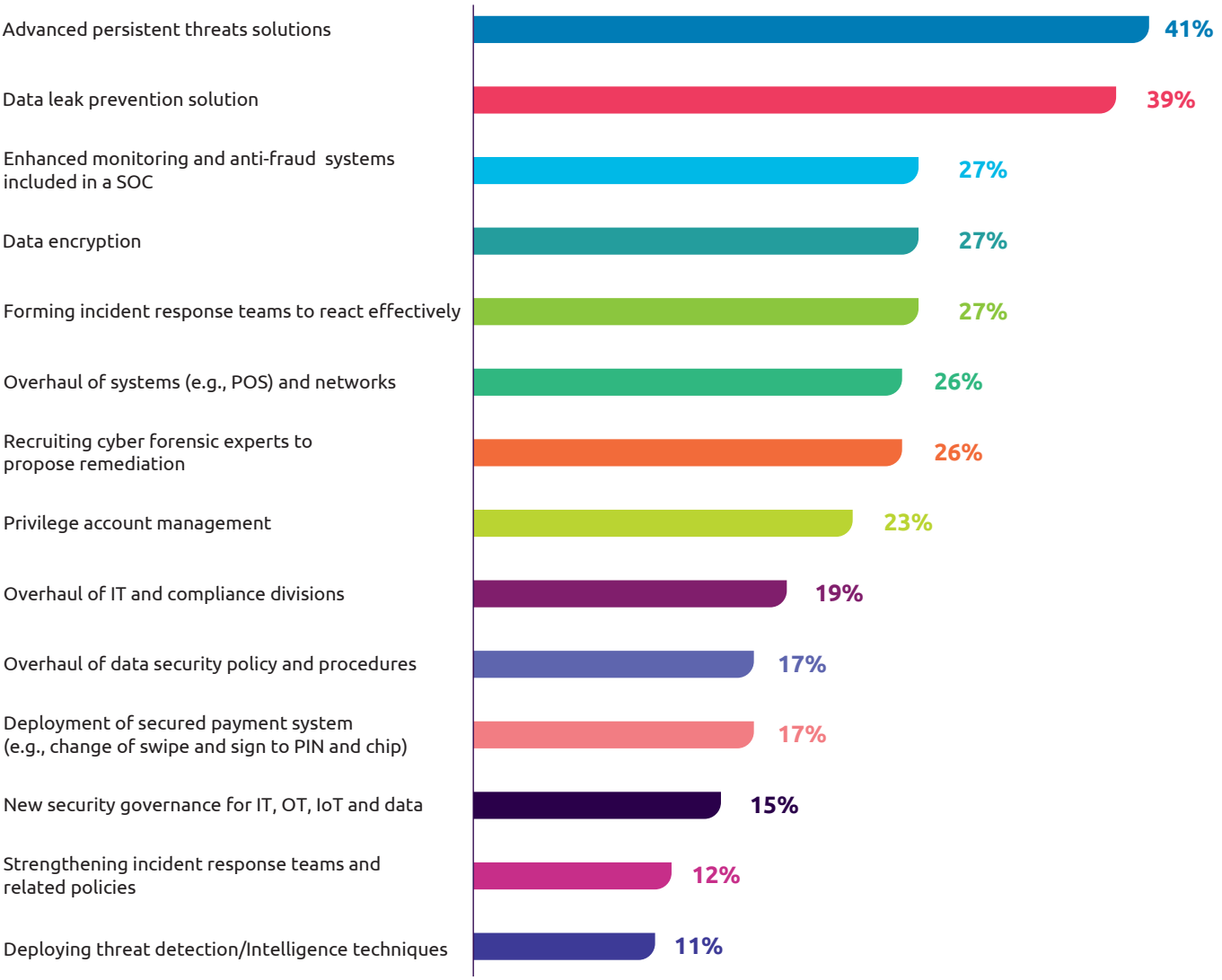
I think the first step is to have a very robust plan that encompasses all of the key elements including the media and public relations response. Ensuring that every level of the organization is aware of the plan and communication so that the salesperson walking the floor in the store will know how to respond when a customer asks a question is imperative."

27%

Retailers who form an incident response team to react effectively after a breach

Figure 18. Retailers most commonly focus on persistent threat detection and data leak prevention after a breach.

Actions taken by retailers post cybersecurity breaches



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

Advanced retailers vs. Beginners

We identified a set of retailers who have fully implemented more than 75% of the cybersecurity and data protection capabilities we studied in this research. They are called "Advanced" retailers and we compare their practices against "Beginner" retailers who have fully implemented less than 50% of the cybersecurity and data protection capabilities.

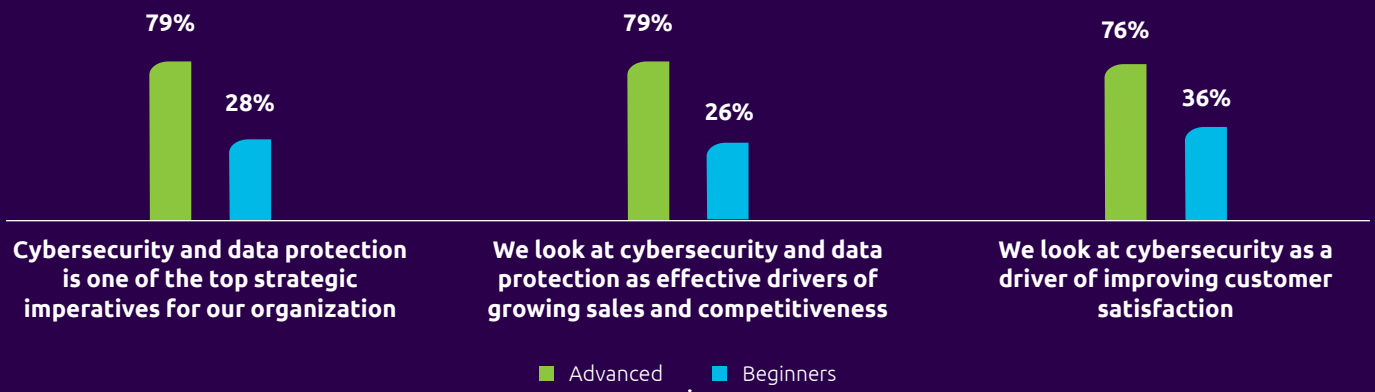
Advanced retailers have implemented more of the cybersecurity capabilities consumers care about

- Safety of stored data… **85% Advanced** vs. **6% Beginners**
- Prompt for passwords while accessing accounts… **87% Advanced** vs. **9% Beginners**
- Clear and transparent data privacy policy… **88% Advanced** vs. **6% Beginners.**

Even if Advanced retailers' systems are breached, the impact on their customers' data is far lower

37% Advanced vs. **71% Beginners** had 25% or more customer accounts compromised.

Advanced retailers prioritize cybersecurity and data protection and look to it for driving growth



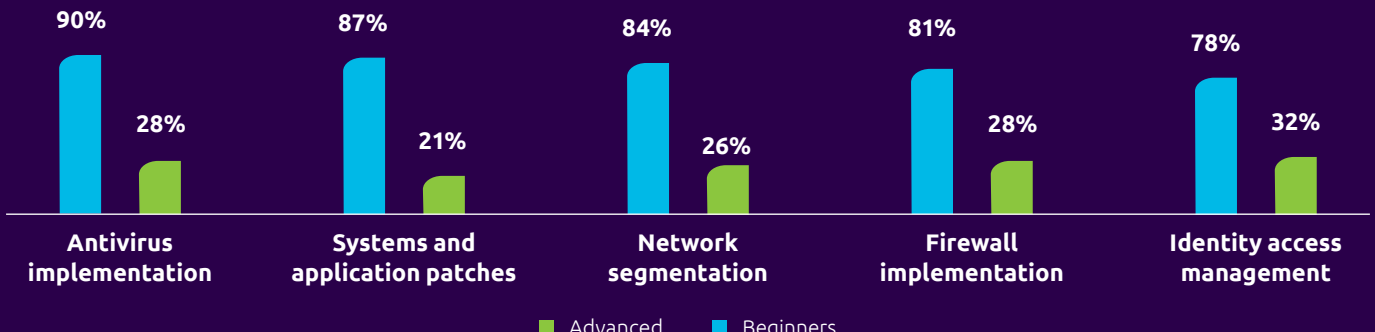
Advanced retailers outspend Beginners on cybersecurity

$259M Advanced vs. **$171M Beginners** average investment across cybersecurity and data protection capabilities

Advanced retailers more frequently involve CXOs in the cybersecurity and data protection agenda

62% Advanced vs. **32% Beginners** say that their CXO is always involved in decisions

Advanced retailers have more frequently implemented the common cybersecurity capabilities



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

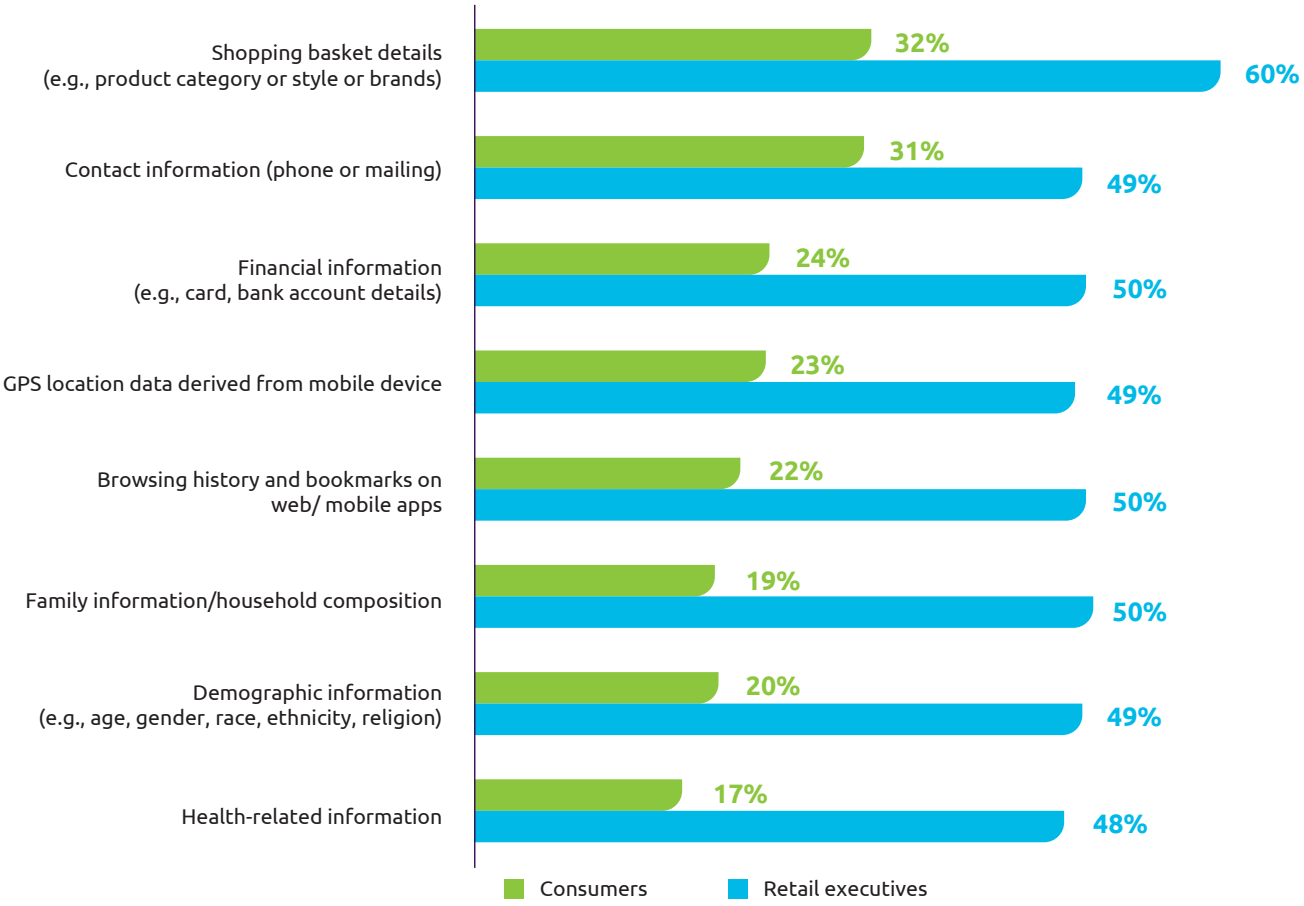
Position yourself as the safe custodian of consumer data

It is clear that consumers take the protection and safety of their personal and financial data very seriously. We found that close to half (48%) say they frequently review the data privacy policies of retailers when they purchase online. However, nearly a third of consumers (29%) say their primary retailer does not communicate data privacy policy changes to them. We also found that only 44% of retailers said that they "assure customers that they are safe custodians of their personal and financial data."

There also appears to be a disconnect between what consumers believe retailers do when requesting their personal data and what retailers say they do (see Figure 19). It is imperative that retailers bridge this disconnect and assure their customers that their data is safe and that the retailer can be trusted.

Figure 19. There is a disconnect between consumers and retailers on whether explicit permission for storing/using data is taken.

Percentage of consumers who say their primary retailer always takes their explicit permission before storing/using their data vs. percentage of retailers who say they always do



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers; N=6,120 consumers.

Soon, with the advent of GDPR, it will not be optional for retailers to ensure they adequately protect and safeguard consumer data. This regulation gives consumers unprecedented levels of rights on the data they share with retailers, such as the right of transfer, erase, and access. Retailers are likely to view the regulation as a compliance burden, however, when implemented in letter and spirit, the regulation could augment cybersecurity and data protection as a "competitive edge" for a retailer than just a checkbox to be ticked.

Of course, retailers still have plenty to do when it comes to implementing certain GDPR requirements, as our survey shows:

- 58% said they have fully implemented the requirement that "terms and conditions of data usage are clearly communicated to customers"
- 55% said they have fully implemented the "right to be forgotten" requirement for customers (i.e., provision to erase customer data when requested by them).

But this leaves around 40% that do not have a fully implemented measure in place yet (see Figure 20). It is important to note that Figure 20 is not an exhaustive list of GDPR requirements and there might be other requirements necessary to be fully compliant with the regulation.

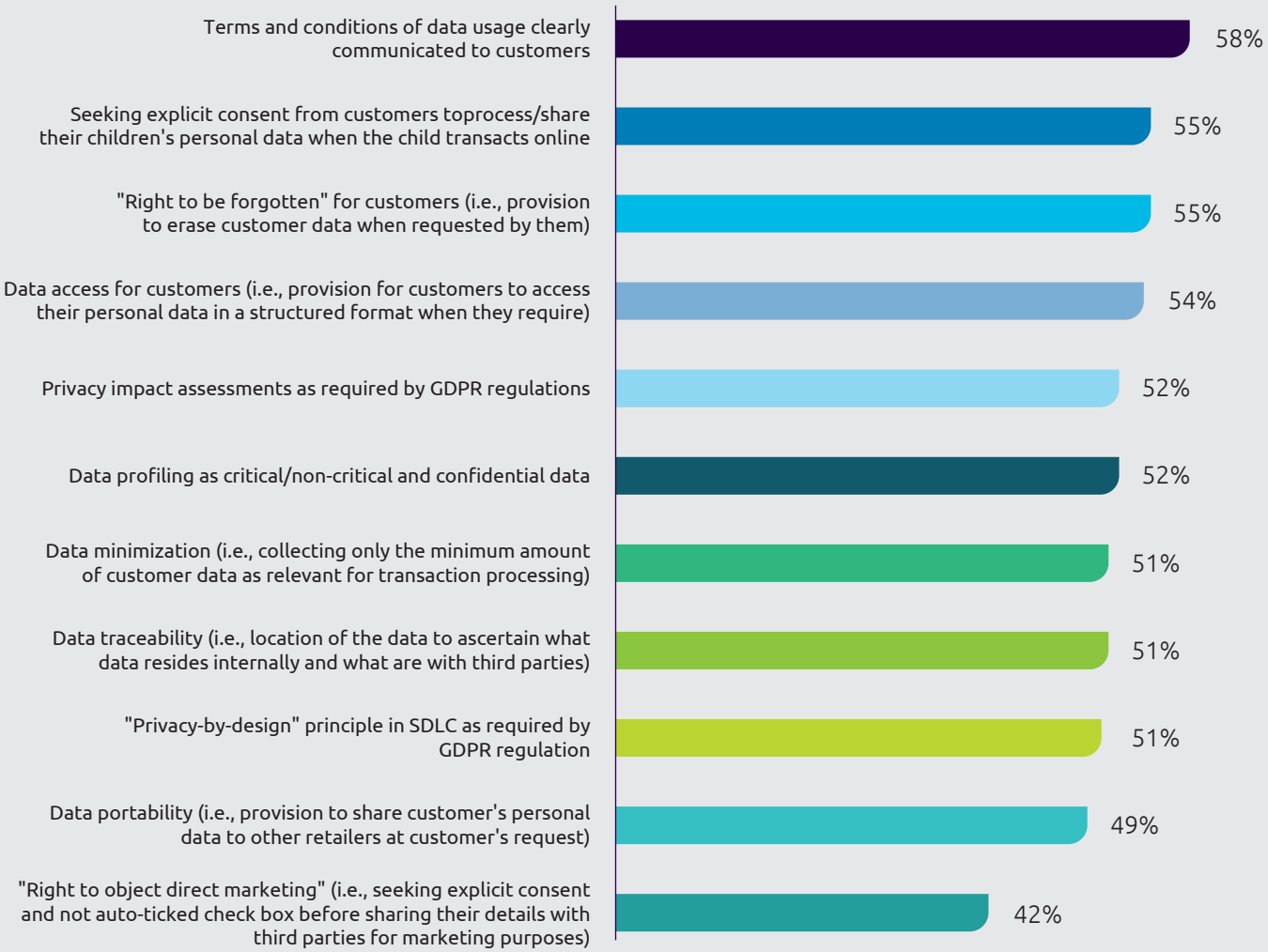
Retailers that are found to be in violation of the regulation will face heavy fines of up to 4% of global annual revenue. Such stiff penalties and reputational damage that might result from non-compliance demand that retailers must make it a top-level priority. UK-based retailer John Lewis, has made GDPR a board-level priority and believes that GDPR presents new opportunities to change organizations' mindset towards consumer data.[11] Steve Wright, John Lewis' group data privacy and information security officer recently said: *"This is changing the way we think of data and how we use it, and giving in to a two-way dialogue with customers which puts them on a much more even footing"* while speaking on the company's GDPR efforts.

How prepared are retailers for the GDPR?

We asked retailers about how their GDPR regulation programs were progressing. As Figure 20 shows, between 40% and 60% said they have fully implemented the required measures.

Figure 20. Forty to sixty percent of retailers have fully implemented certain GDPR requirements

Percentage of retailers who have fully implemented components of the GDPR regulation



Source: Capgemini Research Institute survey, Cybersecurity in Retail; January–February 2018, N=206 retailers.

Conclusion

The traditional perspective that cybersecurity and data protection is an overhead cost needs to change. Our study finds that it is an effective means to gain competitive advantage for retailers since it plays an important role in consumers' minds when they choose their retailers. Cybersecurity and data protection also drives satisfaction and wins consumers' trust. As a result, it can make a positive impact on top-line revenue for retailers. However, retailers in general are missing out on this opportunity, as we found they often lag in identification and implementation of the cybersecurity and data privacy capabilities that matter most to consumers. Retailers who aspire to grow their business, either in-store or online, need to leverage this unexplored dimension.

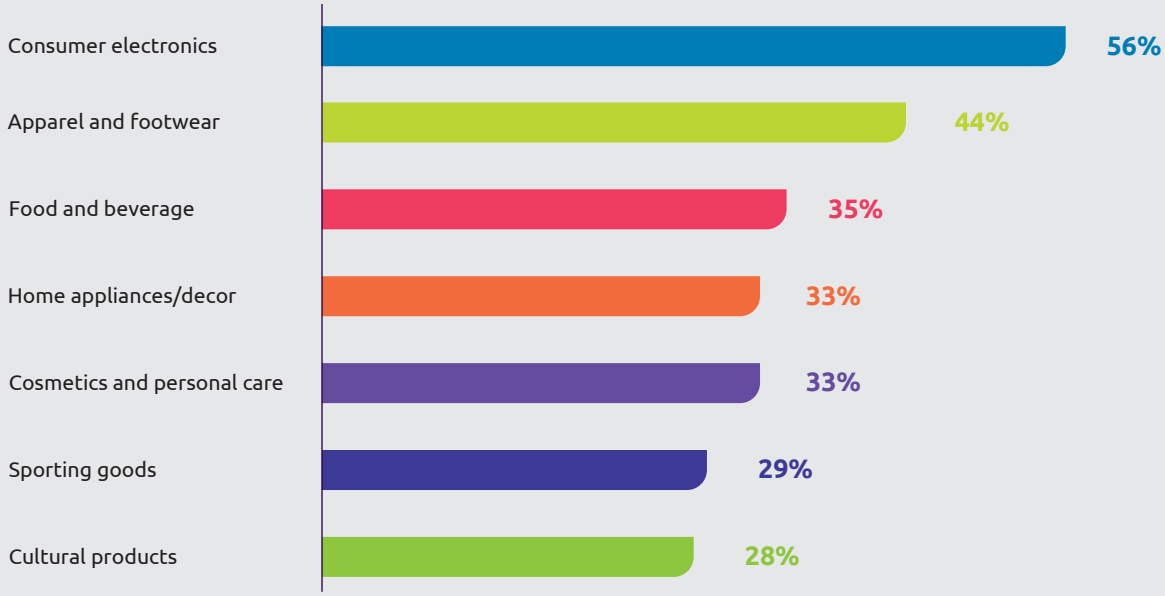
Research methodology

Quantitative surveys:

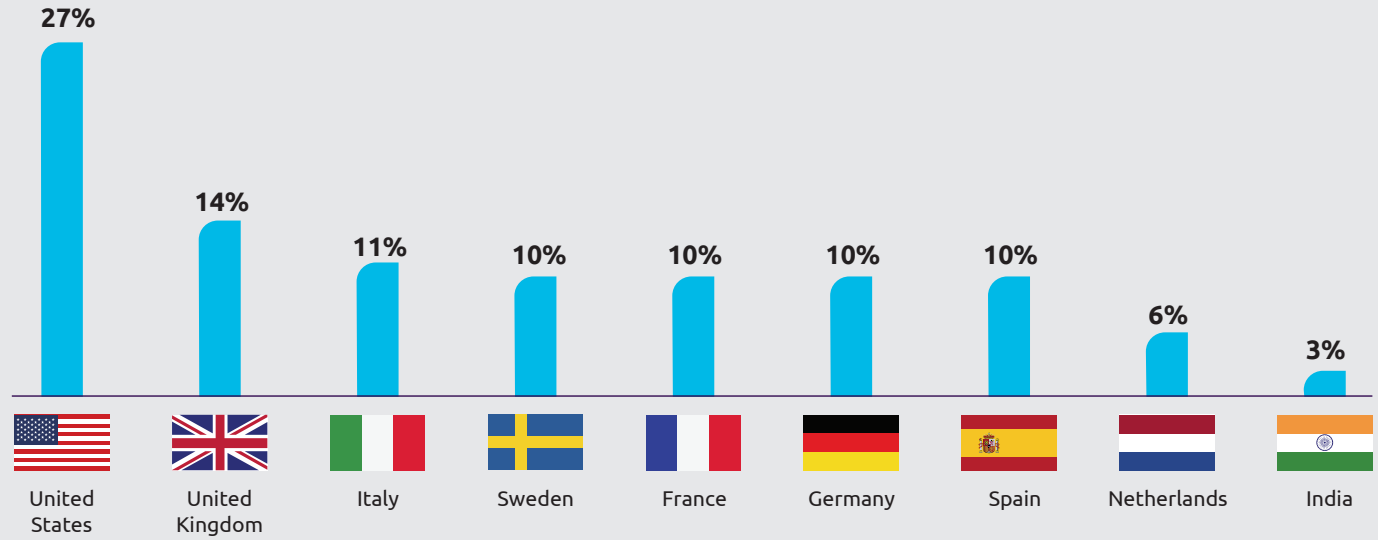
We surveyed 206 executives at the director level or above, with 71% of the executives in retail companies with reported revenue of more than $1 billion in FY 2016. We also surveyed 6,120 consumers aged 18+. Both surveys took place from January to February 2018, and covered nine countries—France, Germany, India, Italy, the Netherlands, Spain, Sweden, the United Kingdom, and the United States. More detail is below.

Country and industry distribution—retail executives

Product categories offered by retailers

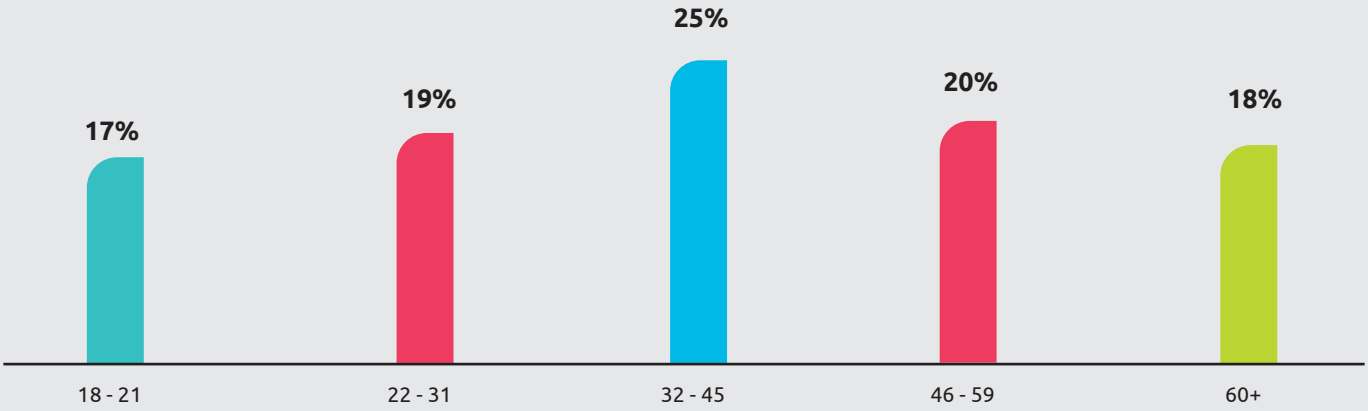


Country of primary residence

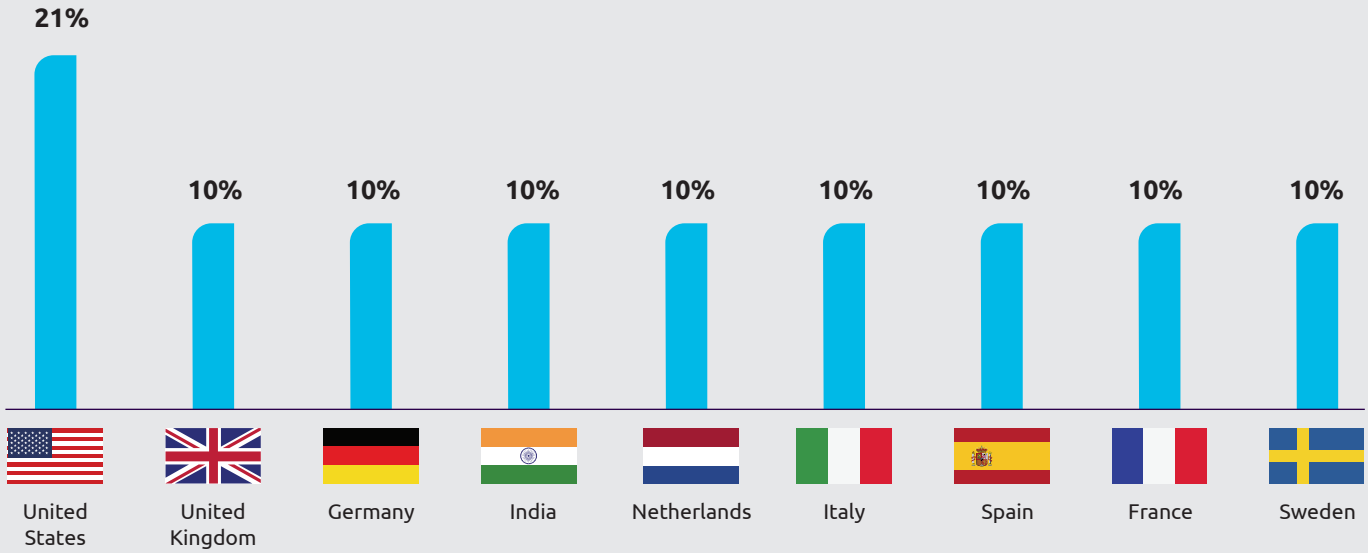


Country and age distribution—consumers

Age Group



Country of primary residence



Focus interviews:

We held 12 discussions with a wide range of senior executives in cybersecurity within the retail sector as well as within security firms specializing in retail, including Chief Information Security Officers, Security Engineers, Cybersecurity Architects, and Information Security Managers. This helped us to understand key challenges in cybersecurity and data protection in retail and identify best practices.

References

1. The Telegraph, "Cyber Attacks on Online Retailers Double in a Year as Hackers Try to Steal Shoppers' Details," August 2017.
2. Information Commissioner's Office, "GDPR, Personal Data Breaches."
3. Capgemini Research Institute, "Loyalty Deciphered—How Emotions Drive Genuine Engagement," November 2017.
4. Out-law.com, "Businesses can obtain a competitive advantage if they get data protection right, says watchdog," August 2017.
5. Independent.co.uk, "Apple launches privacy website intended to show just secure iPhones and other products are," September 2017.
6. Apple Privacy website, Accessed March 14, 2018 https://www.apple.com/privacy/
7. Google Privacy website, Accessed March 14, 2018 https://privacy.google.com/#
8. Econsultancy, "GDPR: How to create best practice privacy notices," July 2017.
9. The cybersecurity budget figure includes planned investment in the next three years across in-house cybersecurity software for network/data protection, cloud-based security solutions, hardware, advanced analytics/machine learning, and employee education and training.
10. In our survey, 86% of consumers said that they would resume shopping at their primary retailer after a cybersecurity breach if the retailer were to send a clear communication detailing under what condition the breach happened, what type of records were affected, what remedial steps have been taken to prevent such a breach in future, and if the impact of the breach on their personal information was low.
11. Digiday.com, "'Biggest danger is apathy': John Lewis data privacy boss on EU data protection laws," October 2016.

About the Authors

Tim Bridges
Global Sector Lead, Consumer Products, Retail Distribution, Capgemini
timothy.bridges@capgemini.com

Tim leads Capgemini's Consumer Products, Retail, Distribution & Transportation (CPRDT) global sector practice, a portfolio that includes major global retail, fashion, restaurant, consumer products, transportation, and distribution brands such as McDonald's, Coca-Cola, Meijer, Office Depot, Domino's, and Unilever.

Geert van der Linden
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

Geert is the cybersecurity business lead of Capgemini's Global Cybersecurity Practice. Prior to this, Geert held roles as CIO of Capgemini's Infrastructure Services Strategic Business Unit (SBU) and Security practice lead in the Cloud Infrastructure Services SBU.

Jerome Buvat
Global Head of Research and Head, Capgemini Research Institute
jerome.buvat@capgemini.com

Jerome is head of the Capgemini Research Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruptions.

Marisa Slatter
Manager, Capgemini Research Institute
marisa.slatter@capgemini.com

Marisa is a manager at the Capgemini Research Institute. Also a manager within Capgemini Consulting North America, she advises clients on customer experience, brand strategy, digital transformation, and digital talent strategy.

Aritra Ghosh
Senior Consultant, Capgemini Research Institute
aritra.ghosh@capgemini.com

Aritra is a senior consultant at the Capgemini Research Institute. He likes to follow how emerging digital technologies are commercialized and what disruptions across industries they bring in.

The authors would like to thank Abirami B from the Capgemini Global CPR Center of Excellence (Crescent) and Kunal Kar from Capgemini Research Institute for their contribution to this report.

The authors would also like to thank Marjorie Daniel from Capgemini Group Marketing, Samir Khare, Erik Hoorweg and Sandeep Kumar from Capgemini Cybersecurity, Kees Jacobs, Marc Rietra, Katja van Beaumont, Steve Hewett and Eloy de Sola from Capgemini Consumer Products and Retail, Jerome Desbonnet and Pierre-Luc Refalo from Capgemini Sogeti Group and Mike Turner from Capgemini Aspire for their contributions to this research.

Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in the United Kingdom, United States and India.

research@capgemini.com

For more information, please contact:

Global

Geert van der Linden
geert.vander.linden@capgemini.com

Tim Bridges
timothy.bridges@capgemini.com

France

Pierre Luc Refalo
pierre-luc.refalo@fr.sogeti.com

Olivier Trouve
olivier.trouve@capgemini.com

Germany

Martin Arnoldy
martin.arnoldy@capgemini.com

Ralph Becker
ralph.becker@capgemini.com

India

Samir Khare
samir.khare@capgemini.com

Aashish Chandorkar
aashish.chandorkar@capgemini.com

Italy

Michela Cotich
michela.cotich@capgemini.com

Netherlands

Erik Hoorweg
erik.hoorweg@capgemini.com

Spain

Carmen Dufur
carmen.dufur@capgemini.com

David Luengo
david.luengo-ruiz@capgemini.com

Sweden

Christer Jansson
christer.jansson@capgemini.com

Fredrik Astrom
fredrik.astrom@capgemini.com

United Kingdom

Sandeep Kumar
sandeep.j.kumar@capgemini.com

Silvia Rindone
silvia.rindone@capgemini.com

United States

Drew S. Morefield
drew.morefield@capgemini.com

Ninad Purohit
ninad.purohit@capgemini.com

Build digital trust with Capgemini's Cybersecurity Services

With 3,000+ cybersecurity experts, Capgemini's cybersecurity team offers a full range of services that safeguard the digital and cloud platforms, IT infrastructures, and OT systems of organizations worldwide. We use the best technology products tested by our R&D team, specializing in malware analysis and forensics. We have ethical hackers, an international network of security operation centers (SOCs), and we are global leaders in testing. We advise. We protect. We monitor.

We offer three families of cybersecurity services:

Governance—Strategic and operational consulting and assessment services that help organizations on a wide range of critical issues. For example, assessing cybersecurity and information protection maturity, developing cybersecurity change management, conducting network penetration testing, and performing security audits. We also partner with organizations to help them prepare for the upcoming GDPR regulation.

- We helped a large US retail corporation develop a target state design for its information security organization, given its future cybersecurity challenges and ambitions.

Protection—Dedicated or managed security services designed to stop advanced threats with an integrated security architecture. Our security services' framework includes four key components: endpoints, apps, identity and access management and infrastructure. We also specialize in protection services for the public cloud.

- We supported a European supermarket chain to define an access management architecture and create an identity and access management strategy that allowed them to better plan deployments and streamline access provisioning.

Monitoring—Gaining visibility of your IT and security system to detect, analyze and react to cyber-attacks. We help organization detect and analyze even the most advanced attacks before they can impact the business. Through our dedicated and managed security services, we offer incident detection, incident response and reporting, and incident prevention.

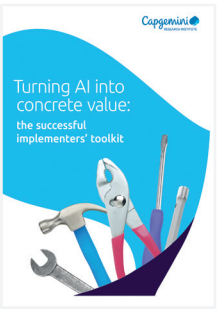
- We helped a European automobile manufacturer set-up a security operations center to monitor up to 30,000 events per second, detect attacks earlier and react proactively.

Learn more about our services at
https://www.capgemini.com/service/new-ways-to-control-secure-your-assets/

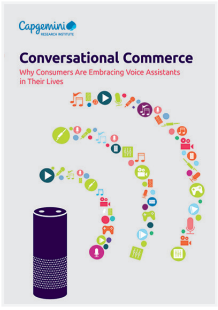
Discover more about our recent research on digital transformation

Cybersecurity Talent: The Big Gap in Cyber Protection

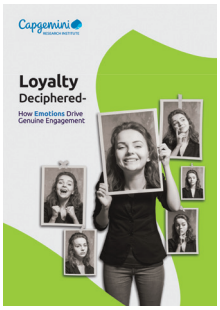
Digital Transformation Review 11: Artificial Intelligence Decoded



Turning AI into concrete value: the successful implementers' toolkit



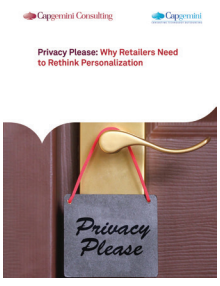
Conversational Commerce: Why Consumers Are Embracing Voice Assistants in Their Lives



Loyalty Deciphered: How Emotions Drive Genuine Engagement

Making the Digital Connection: Why Physical Retail Stores Need a Reboot

The Digital Culture Challenge: Closing the Employee-Leadership Gap



Privacy Please: Why Retailers Need to Rethink Personalisation

The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com

People matter, results count.