Capgemini Consulting

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

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

By the Digital Transformation Institute

Executive Summary

Are retail banks and insurers a safe pair of hands when it comes to customer data? Our global survey of more than 180 senior data privacy and security professionals—as well as 7,600 consumers—found that less than a third (29%) of these organizations offer both strong data privacy practices and a sound security strategy. In fact, just one in five (21%) organizations are highly confident that they can detect a cybersecurity breach.

This picture has so far not unduly affected consumers' perceptions of the industry. We found that 83% of consumers trust banks and insurers when it comes to data. And while one in four institutions have reported being the victim of a hack, just 3% of consumers believe their own bank or insurer has ever been breached. However, with the pending General Data Protection Regulation (GDPR), this trust factor is likely to change as transparency increases. Financial organizations have to reveal a data breach within 72 hours after the incident.

Banks and insurance firms have a clear incentive therefore to fortify their defenses. As well as avoiding the prohibitive fines and penalties that will result from compromised data, protecting privacy offers a strategic business advantage. Addressing security concerns will drive greater adoption of low-cost digital channels. We found that security concerns deter nearly half of consumers (47%) from using digital channels. It will also reduce churn and attract competitors' customers – 74% of consumers would switch their bank or insurer in the event of a data breach.

Preparing to be a trusted data steward is no easy task, however. It means raising the bar on multiple dimensions:

- Aligning data practices with consumers' expectations
- Finding innovative ways of providing non-intrusive security to consumers
- Building the capabilities required to monitor cyber risks on a real-time basis
- Revisiting the data governance model.

Building your reputation for data privacy and robust security is definitely challenging. But, those who strike the right chord with consumers will enjoy a competitive advantage over their peers and come out triumphant in the trust game.

More than two-thirds of organizations are not prepared to be trusted stewards of consumer data

2016 was not a great year for data breaches, regardless of what sector you were in[1]. In the US, for instance, it was a year where the number of breaches reached record levels. In this compromised environment, we set out to understand how consumers view the security and data privacy practices of financial institutions. And, of course, to understand how these institutions can remedy the situation and become trusted stewards of consumer data. We surveyed 7,600 consumers across eight countries, and also interviewed 183 senior security and privacy professionals from global banking and insurance organizations (see research methodology at the end of the document).

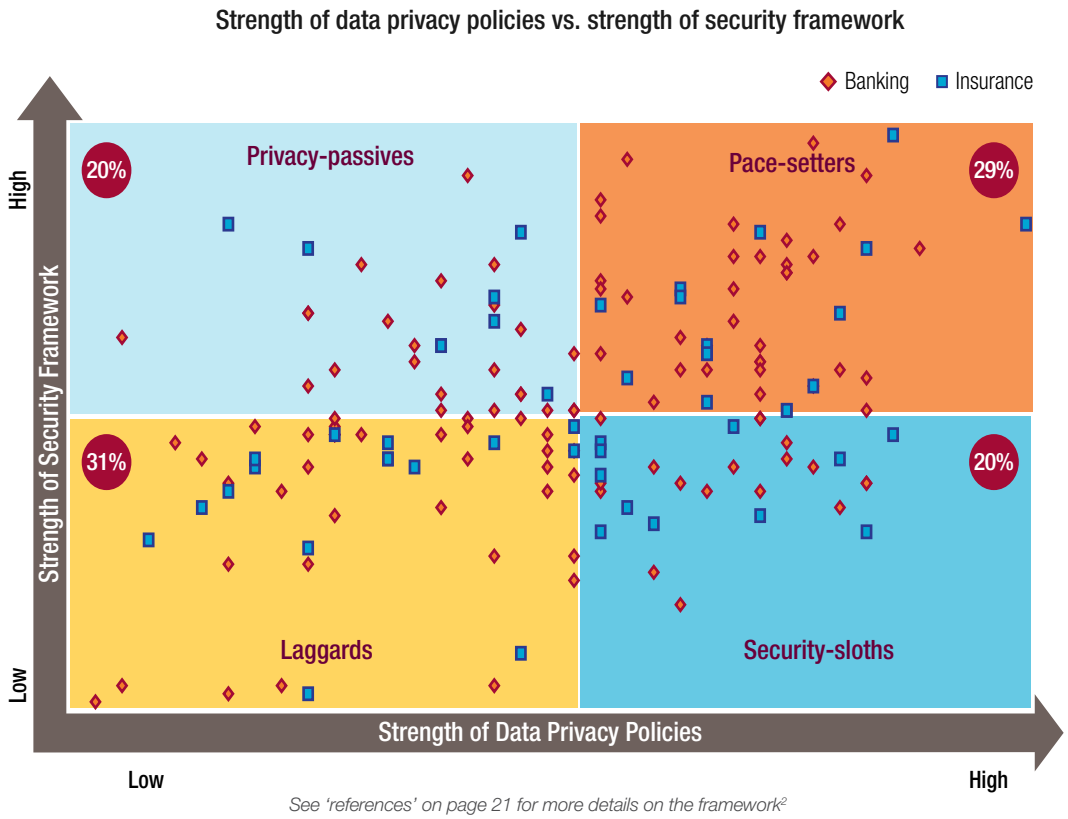
29% of organizations have both strong data privacy policies and sound security frameworks

One in two banks and insurers have inadequate data security frameworks or privacy policies

The results from our survey of industry executives do not paint a very flattering picture of security and privacy practices. We see four categories of players emerging (see Figure 1):

- **Pace-setters** – Have a highly-compliant data privacy policy backed up with a best-in-class security strategy.
- **Security-sloths** – Have a fairly strong privacy policy but relatively weak security strategy.
- **Privacy-passives** – Have a highly-secure data environment but lag in terms of implementing strong data privacy practices.
- **Laggards** – Have only basic data privacy and security tactics in place across the enterprise.

Figure 1: How are the banking and the insurance organizations characterized regarding data privacy and cybersecurity?



See 'references' on page 21 for more details on the framework[2]

(N=163) Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

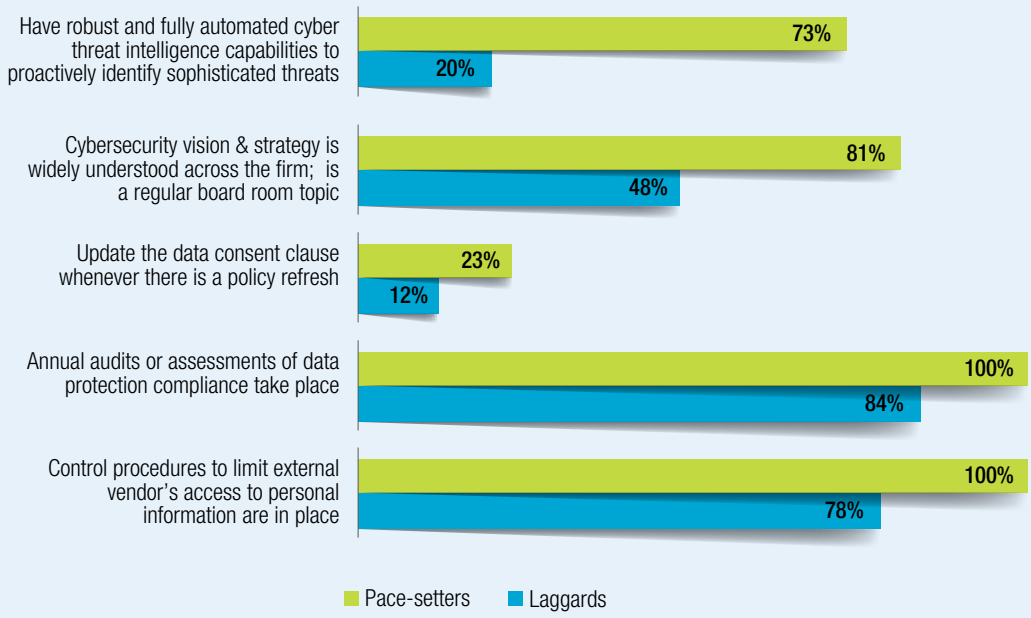
**While the survey covered 183 institutions, only 163 out of these, responded for both the data privacy and cybersecurity parts of the survey, and so have been considered for developing this framework.*

What sets 'Pace-setters' apart?

Pace-setters:

- Have a sophisticated security intelligence program complementing their breach detection ability
- Are better prepared to respond to a potential data hack
- Show greater participation and support from the board on cybersecurity matters
- Have better data practices compared to other banks and insurance organizations: audit and compliance, strong controls for data access, and governance.

Figure 2: How Pace-setters outrank Laggards



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

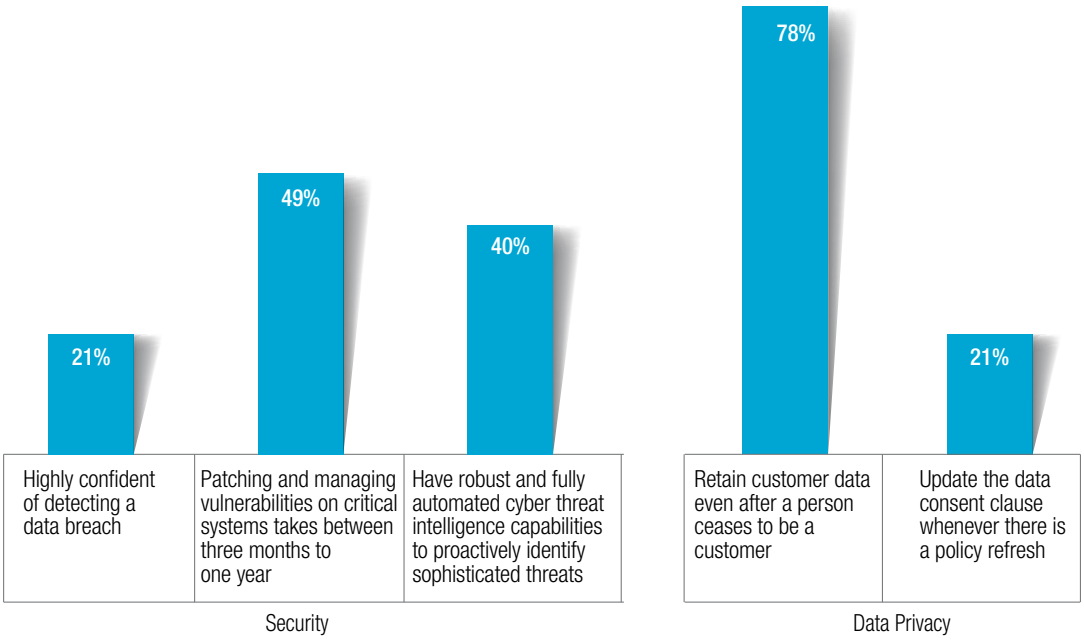
Where are banks and insurance organizations lagging?

Breach detection and management is inadequate

Only a few institutions have a sophisticated ability to identify cyber attacks and manage risks. As Figure 3 shows, only one in five institutions (21%) are highly confident about their ability to detect a breach. This is a worrying sign given the potential business impact. As Christopher Graham, the UK's Information Commissioner, says, "The knock-on effect of a data breach can be devastating. When customers start taking their business elsewhere, that can be a real body blow.[3]"

Nearly half of financial institutions (49%) take a long time to patch and manage vulnerabilities— from three months to one year. The more time it takes to patch vulnerabilities, the higher the risk of critical systems being compromised. This is because around half of all exploitation attempts by attackers occur within 10 to 100 days[4].

Figure 3: How financial services organizations fare on key security and privacy parameters



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Only 40% of organizations have fully automated cyberthreat intelligence processes

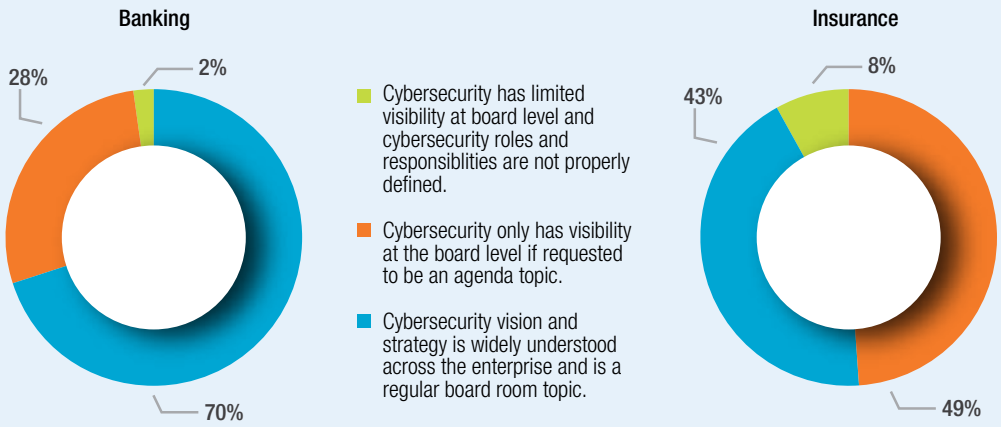
Security intelligence processes are missing the mark

Breach detection controls would be significantly improved if they were backed-up by coordinated and automated security intelligence systems. However, only 40% of organizations said they had fully automated cyberthreat intelligence processes capable of proactively identifying sophisticated threats. Instead, organizations are relying on manually patching together data from a wide variety of sources to create the necessary intelligence. As a result, response times lengthen and risk increases. As attacks grow in complexity, precision, and volume, manual approaches to comparing external and internal intelligence feeds are no longer adequate. A fully automated threat intelligence system enables banks and insurance companies to analyze and understand threats and prioritize risk on a real-time basis.

Insurers lack governance and control

Our multi-year research into the principles of successful organizational digital transformation has consistently pointed to the importance of strong leadership support from the top. However, if we apply that principle in the context of cybersecurity strategy, the results are disappointing. We found that the boards of insurers are playing a passive role when it comes to defining cybersecurity strategy. Less than half of insurance companies (43%) can point to a board that actively participates in cybersecurity matters, with a clearly articulated cybersecurity vision and strategy (see Figure 4). This lags banks significantly, where 71% of organizations have board involvement.

Figure 4: We have a widely understood cybersecurity vision and strategy and it is a regular board room topic



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Privacy practices need to be strengthened

Banks and insurers also need to do more to build a reputation for strong data privacy practices (see Figure 3):

- 78% retain data after a customer has exited the relationship, of which 62% retain it for as much as ten years after the customers have left
- Only 21% updated the data consent clause in the privacy policy during a policy refresh.

The General Data Protection Regulation (GDPR) lays down key conditions[5] for lawful and transparent processing and retention of data by organizations. The regulation, for example, mandates informed and unambiguous consent as one of the conditions for processing data. (For a detailed analysis on preparedness by country, please see: "How prepared are banks and insurers for GDPR?")

Only a third

of the organizations have made strong progress in implementing GDPR guidelines

How prepared are banks and insurers for GDPR?

The GDPR, which comes into force in May 2018, includes a range of important user rights (some of which already exist): right of deletion, right to be forgotten, right to portability or more stringent conditions to obtain consent from data subjects. Organizations that fall under the purview of GDPR will need to make significant adjustments to their operations, data management policies and governance structures. They will need to evaluate their data-sharing processes to accommodate all the new requirements, particularly in relation to guidelines such as privacy-by-design, reporting breaches, lawfulness of processing personal data and data portability.

While compliance will be essential, among executives surveyed only a third (32%) described their organization as having made strong progress in implementing the requirements of the GDPR guidelines.

The European nations are more prepared than the US. This is not surprising, given that the main principles of privacy law are already applicable under the current EU Data Protection Directive and some countries have already implemented laws that embody certain provisions of GDPR. For instance, the UK's 2007 Data Protection Act has a provision for banks and insurers to report data breaches to the local data protection regulator[6]. Since 2001, Germany has mandated the appointment of a Data Protection Officer[7].

The perception gap – consumers are not aware of the sector's security weaknesses

Banks and insurers enjoy a perception advantage: consumers currently believe they have fortress-like digital security. But as transparency about breaches is set to increase, how long will this positive perception last?

Many consumers still view banks and insurers as largely impenetrable. Only 3% of consumers said that their bank or insurer had been subjected to a cyber-attack or a data breach in the last 12 months. However, 26% of organizations said they had been the victim of a hack (see Figure 5).

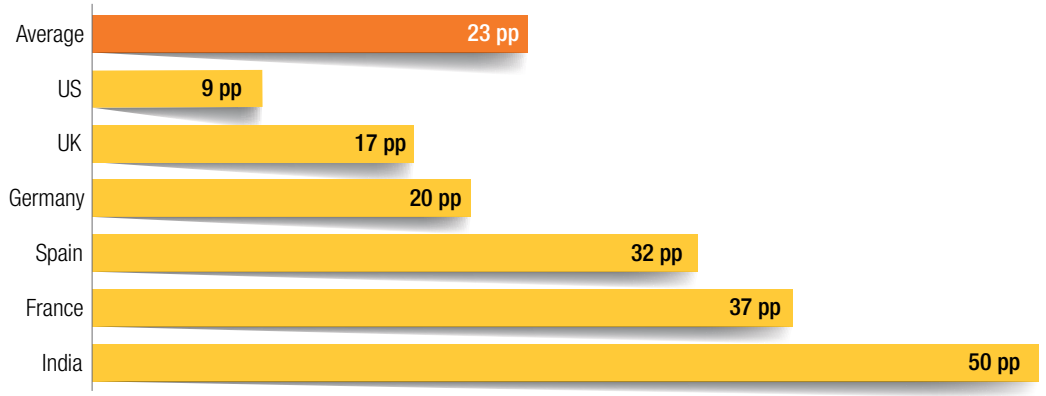
Figure 5: The perception gap between actual occurrence of cyber attacks and what consumers know

Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

3% of consumers believe that their bank or insurer has experienced a data breach

As Figure 6 shows, this perception gap varies across countries, with the most pronounced difference in India (50% perception difference) and the smallest in the US (9%). In India, the lack of consumer awareness can be partly explained by the fact that the concept of data privacy and protection is at a very nascent stage and no guidelines on reporting of data breaches exist. In comparison, the US has stricter federal regulatory guidelines on how financial organizations must notify consumers of breaches, increasing consumer awareness.

Figure 6: Geographical differences in perception gap between consumers and institutions on cyber-attacks (percentage point - pp, indicates the extent by which customers' perception falls short of reality)



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

The perception gap explains why consumer trust in banks and insurers is high

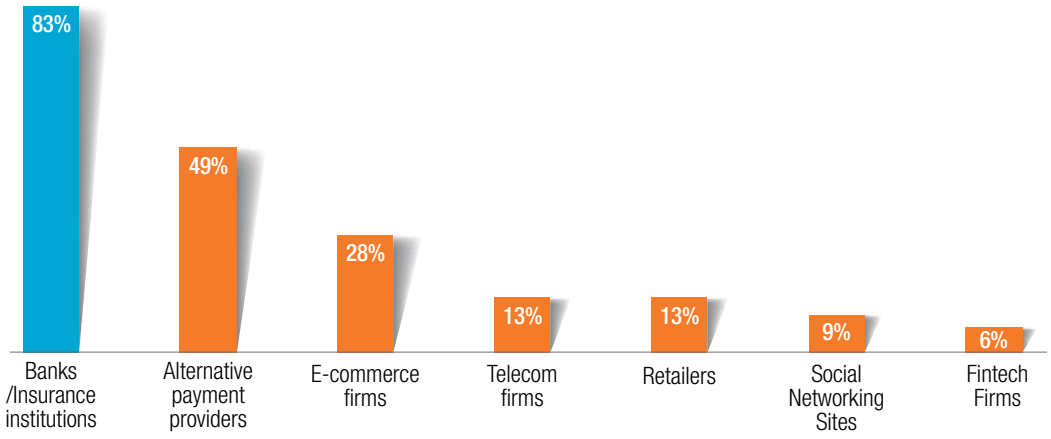
Consumers' lack of awareness might explain the high levels of trust they have when it comes to handling personal data. As Figure 7 shows, we found that 83% of consumers consider banks and insurers trustworthy, significantly outperforming other sectors such as retail or telecommunications.

The level of trust placed in banks and insurers is consistently high across all age groups:

- 78% for Millennials (aged 18 – 34)
- 82% for Gen X (aged 35 – 54)
- 88% for the baby boomers and the elderly (55+)

83% of consumers consider banks and insurers trustworthy

Figure 7: Trust in financial institutions is significantly higher than for other sectors



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

However, this positive perception is under threat. With the new GDPR regulations mandating that banks and insurers report a breach within 72 hours, consumers might discover that banks and insurers are not the fortresses they thought they were[8].

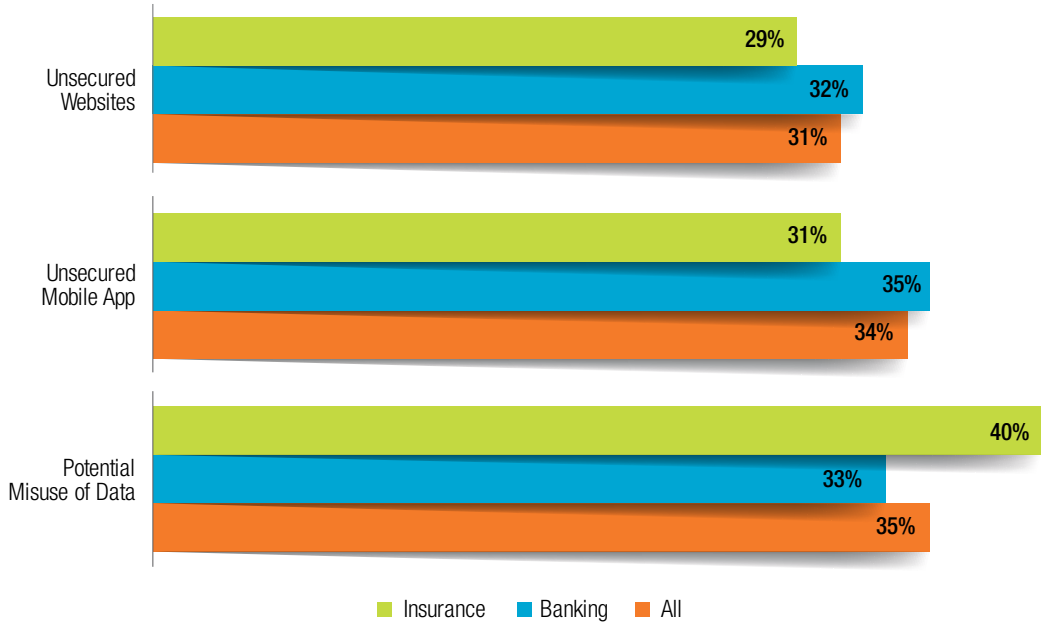
The benefits of getting security and privacy right

Addressing security concerns will drive greater adoption of low-cost channels

Our research shows that security concerns deter nearly 47% of consumers from using digital channels. These consumers are primarily deterred by the prospect of misuse of personal data, followed by a lack of confidence in mobile apps (see Figure 8). Addressing security concerns would help attract more consumers online. It would also help reduce distribution costs, since transaction costs are estimated to be 43 times greater in a branch than via a mobile channel[9].

74% of consumers would switch their bank or insurer in the event of a breach

Figure 8: Primary reasons for not using a digital channel

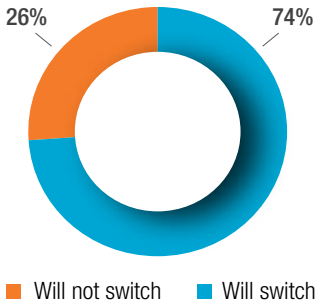


Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Reducing churn, and attracting customers from competitors

Banks and insurers with strong security and privacy practices can set themselves apart from competitors by winning consumer trust —65% of consumers in our survey consider privacy and security as extremely important when choosing their banks and insurers. Organizations with greater levels of trust will be in a strong position to attract the high number of customers that say they would leave their organization in the event of a breach. We found that 74% would switch their bank or insurer (see Figure 9).

Figure 9: Proportion of consumers who would switch in case of a data breach

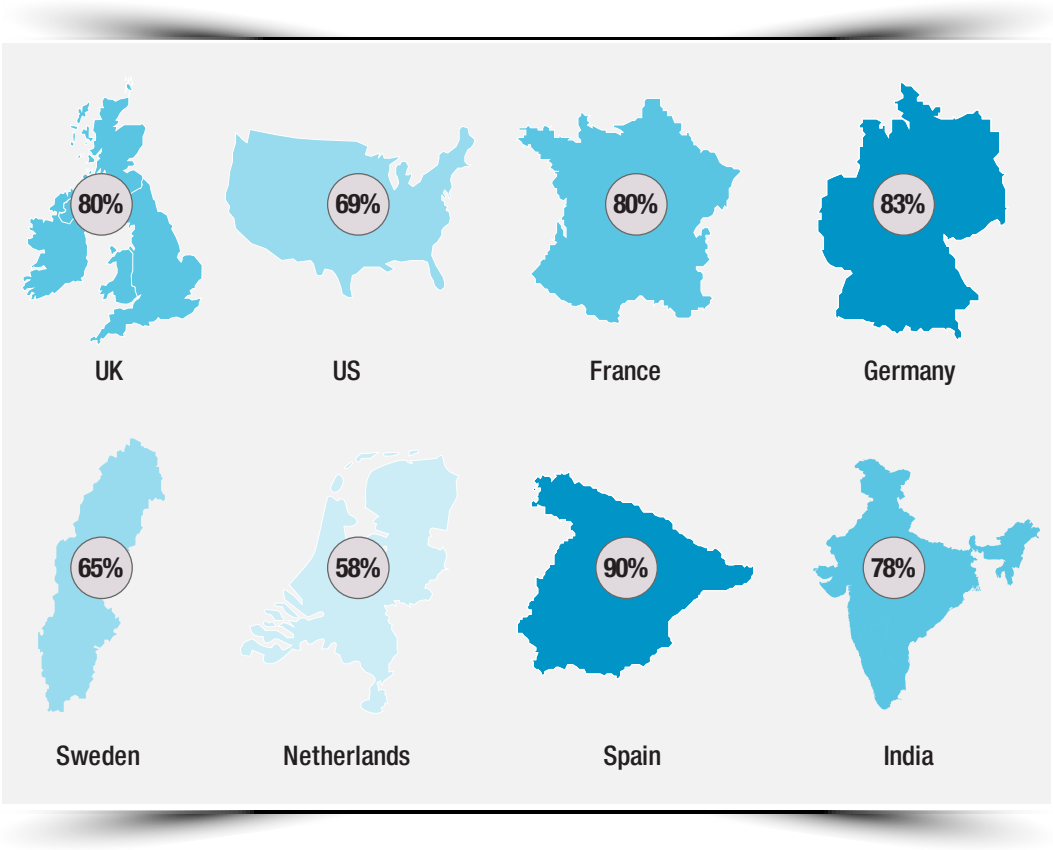


Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

This sentiment is consistent across all ages —millennials, Gen X, baby boomers and the elderly— and also countries surveyed. Potential churn reaches 90% in Spain, 83% in Germany and 80% in France (see Figure 10). The high percentage of banking consumers attacked by malware in Spain might help partly explain customers' greater willingness to switch in the event of a data breach[10].

90%
of consumers in Spain would switch bank in case of a data breach

Figure 10: Likelihood to switch across geographies

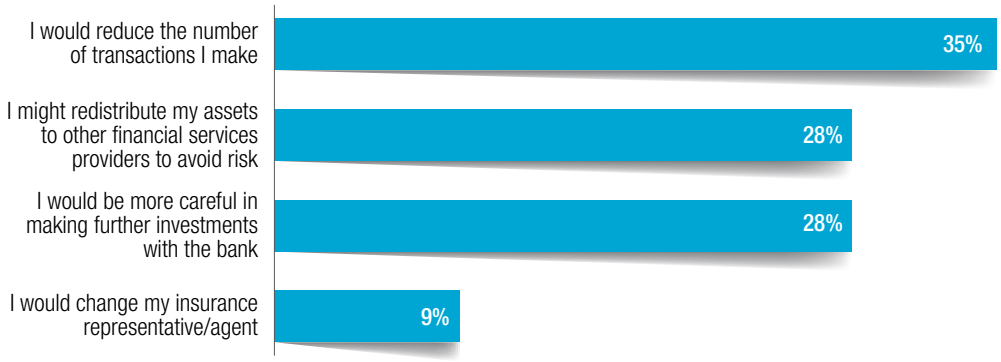


Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

In a real-life scenario, customers may be less swift to actually switch, potentially put off by the cost and the inconvenience of switching providers. However, even if only a small percentage of consumers act and move to a competitor, it could significantly impact the firm.

Financial institutions that deploy best-in-class security and privacy practices will be better positioned to win over customers from competitors. They will also be better placed to alleviate the concerns of consumers following a breach: over a quarter of customers would be cautious about further investments or would redistribute assets to competing financial institutions or non-financial new entrants (see Figure 11).

Figure 11: Impact of data breach on transactions



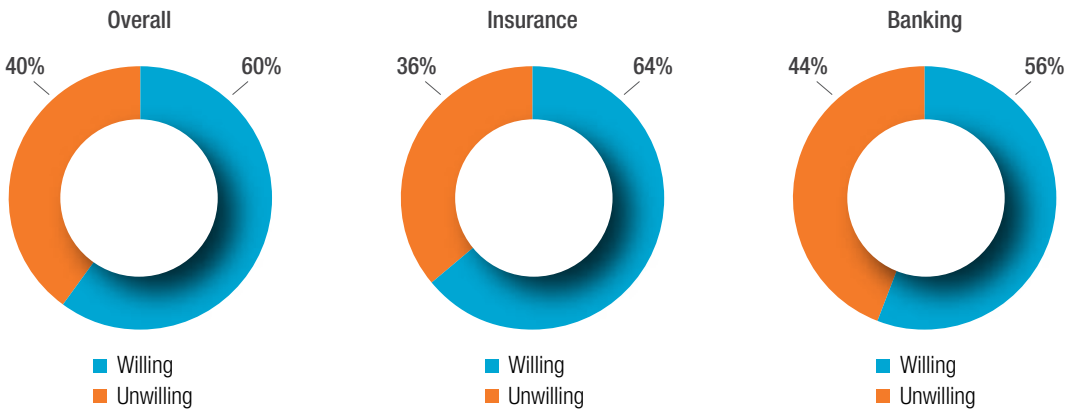
Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

60% of consumers are willing to trade privacy in return for benefits

Earning trust will encourage greater data-sharing

Financial institutions that enjoy a high degree of consumer trust will see more consumers willing to trade privacy in return for benefits. As Figure 12 shows, this was true of 60% of consumers in our survey. While sentiment varies by age and nationality (see "Willingness to trade differs by age and nationality"), there is a clear opportunity for banks and insurers to offer personalized and targeted offerings. Some organizations are already making rapid strides. For example, multiple home insurers in the US are reducing their business risk by monitoring data from safety devices installed in consumer homes. In return for this exchange of data, consumers are being offered discounts on home insurance premiums. Transparency in the use of data by insurers –-and the freedom to opt-in or opt-out of the deal—helps build trust and creates a win-win situation for bothh.

Figure 12: Willingness to trade personal data in return for benefits



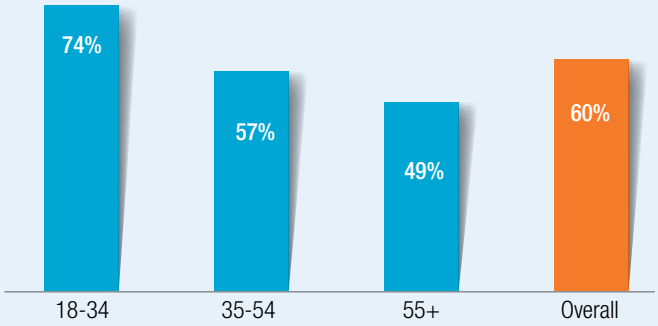
Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Willingness to trade differs by age and nationality

Millennials stand out from other cohorts

Millennials (aged between 18 and 34) are the most willing to share personal data among all age-groups.

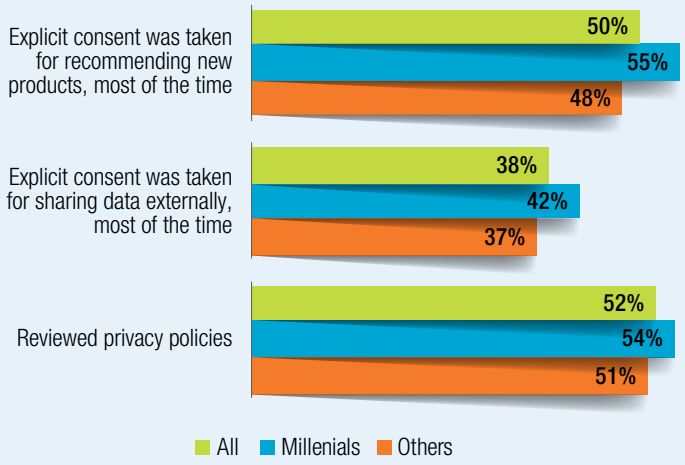
Figure 13 : Willingness to share personal data



Source : Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

As Figure 14 shows, their awareness of organizations' data practices might explain their higher propensity to share data.

Figure 14 : Millennials are more aware of their data than other age groups



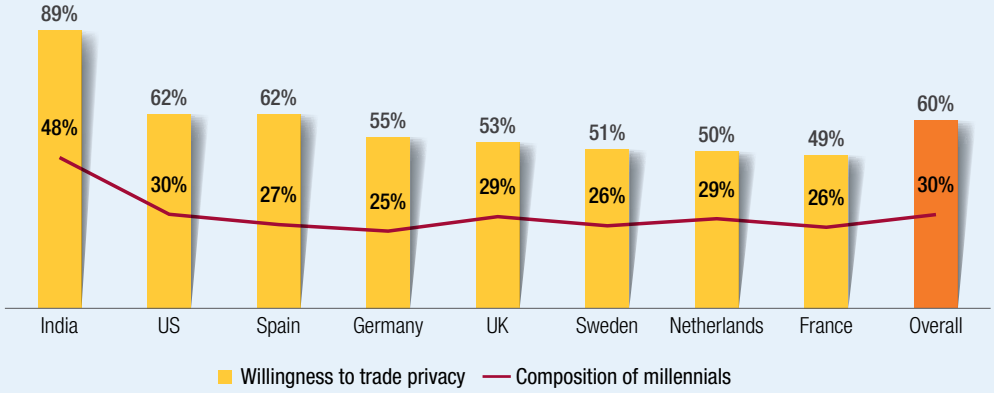
Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Baby boomers and the elderly have high levels of trust but are unwilling to share data

Baby boomers and the elderly are the most unwilling to share data with banks and insurers. Their reluctance to trade data can perhaps be linked back to their past experiences: 45% of consumers in the 55+ age group felt that their bank or insurer never took explicit consent from them while using data internally or when shared with third parties. Not seeking consent in explicit ways could be a potential deal breaker for this segment.

As shown in Figure 15, a combination of cultural nuances and the number of millennials in each country might help explain the disparities in data sharing across countries.

Figure 15 : The willingness to trade privacy in return for services also varies across countries



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

How can financial institutions stay secure, and trustworthy in an insecure world?

21% of consumers never changed their login passwords

Apply a consumer lens to define data privacy and security policy

Financial services organizations need to revisit their data usage and protection strategies through the lens of the consumer. As an executive recently told us: "Privacy needs to be as defined by the customer, not the company."[11]

A number of steps will be critical to bring data practices in line with what consumers want:

Give customers more control: Banks and insurers need to make the ground rules of data sharing very clear. This means giving consumers the choice of opting-in for the data they feel comfortable exchanging. The GDPR already mandates clear and explicit consent as one of the conditions for processing data and banks and insurers will be forced to cede more control on their personal data to consumers[12]. Those organizations that are able to do it sooner, and proactively, will be rewarded with greater trust and higher willingness to share data.

Communicate sooner and more clearly: One aspect that stood out from our research was an un-addressed consumer need for prompt communication. An overwhelming majority of consumers (85%) want either instant communication or to be notified within one day of a breach. Likewise, 40% of consumers feel that their financial institution did not communicate any changes to privacy policy after a breach. This could have serious implications on how their data practices are viewed. As Helge Veum, Deputy Director of Inspectorate (Norwegian data protection authority), puts it: "Even where the individual cannot take action following exposure of their personal data, we deem there is a right to know which deserves protection[13]." Financial services organizations also need to ensure that they have a sound communication strategy in place for any changes in their policies and, most importantly, in case a data breach takes place.

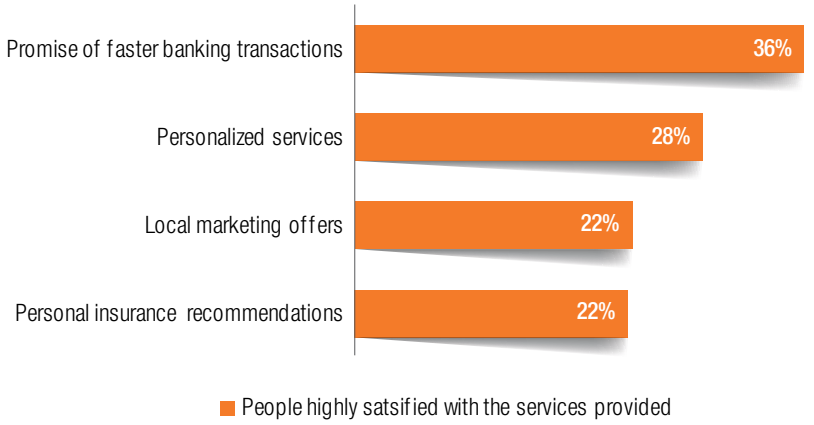
Educate customers on security issues: While consumers are very concerned about security breaches, their own actions do not always match the level of concern. In our survey, 43% of consumers did not report the loss of a credit card immediately after the incident, and one in five consumers (21%) never changed login passwords of their banking/insurance accounts. These behaviors indicate that there are consumers who have a lackadaisical attitude to security. They expect their banks and insurers to shoulder the responsibility of securing their data rather than taking individual responsibility. It also raises a vital question about whether consumers fully understand the risks associated with these behaviors.

Provide more value for data exchanges

Our research shows that consumers are broadly unhappy with the value they get out of exchanging their data (see Figure 16):

- Only 22% are highly satisfied with the services provided as part of local marketing offers and personal insurance recommendations
- Just 36% of consumers are highly satisfied with the promise of faster banking transactions

Figure 16: Consumers who are highly satisfied with services offered in exchange for sharing data



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Over a third of consumers are ready to pay for enhanced security

Banks and insurance companies need to redesign the value proposition that they are currently offering to consumers. A good starting point would be to carefully analyze what consumers value and what they do not. We observed that when a consumer finds value in the services they consume, their willingness to treat data as a tradable asset goes up (see Figure 17). For example, willingness to share data was higher for "lower pricing on insurance products" (52%) as this option offers more direct tangible benefit to the consumer compared to "targeted investment offering" (30%).

Figure 17: Willingness to trade privacy in relation to value received

Benefits received in exchange of data	Value to consumer	Value to banks / insurers	Willingness to share data
Lower pricing on financial products (for e.g. lower insurance premium based on a better health profile)	Very Strong	Very weak	52%
Faster and more secure access	Strong	Weak	47%
Personalized financial planning advice based on your age and spending profile	Moderate	Moderate	37%
Targeted investment/product offers based on your location and/or occurrence of an event such as marriage or birth of a child	Weak	Very Strong	30%

Very weak · Weak · Moderate · Strong · Very Strong

Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey, Capgemini Analysis

One in four consumers are prepared to use some form of biometrics

Simplify and clarify privacy policies

The idea that most users do not read privacy policies is a common belief. But it is only true in part. In our research, while we did find that nearly half of consumers (48%) have never reviewed privacy policies, of which 40% would actually like to do so. However, one issue holding them back is the way privacy policies are cloaked in legalese. Privacy policies should be simple enough for consumers to understand and transparent enough to help build trust. While compliance requirements mandate the use of legal wording, a plain English version of the privacy policy and how it impacts consumer data is helpful. The more consumers understand how their data is being collected, stored and used, the more they will be willing to share data. Some points that banks and insurers can look to include in their privacy policies are:

- What types of personal data are collected by the firm?
- How is the data being used?
- What are the opt-in and opt-out options available to the consumers?
- What practices does the firm have in place to protect the data?
- What benefits do consumers get in return for sharing data?

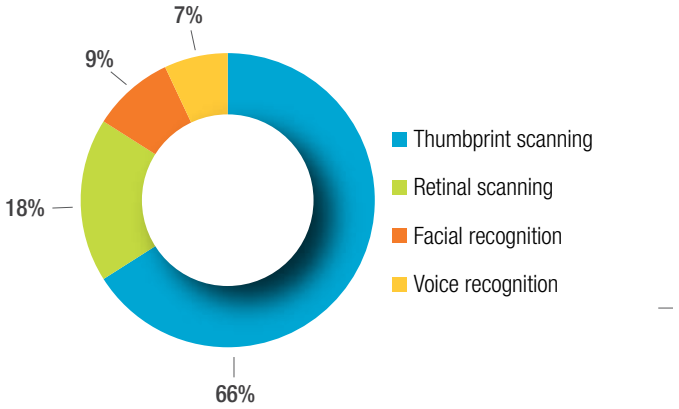
The task does not end here. Banks and insurers also need to review their privacy policies at periodic intervals to ensure that it is in sync with changing regulations. Any changes to privacy policy should also be communicated to consumers as soon as it is implemented.

Provide non-intrusive security using biometrics

The growing incidence of fraud, and increasing complexity of malware attacks, will require financial institutions to adopt a multi-tiered approach to security. Investments need to be made in new security technologies such as tokenization, biometrics and end-to-end encryption. One area that has seen considerable traction recently is biometrics. It is already being used by large banks globally to allow consumers to check account balances and make payments and there are encouraging signs that consumers are receptive to it:

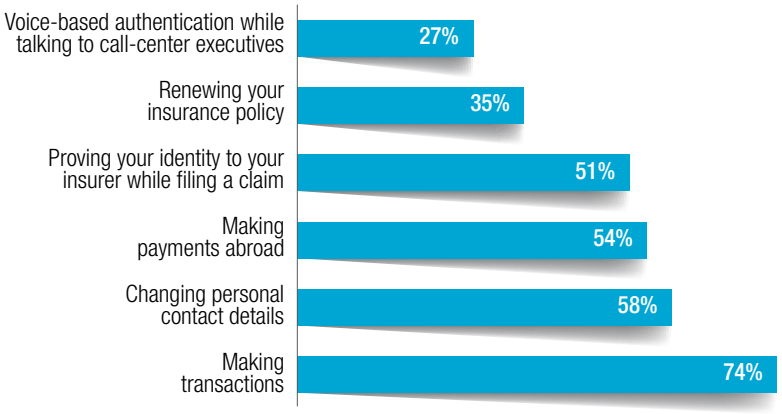
- A quarter of respondents in our survey are prepared to use some form of biometrics in accessing their account, with thumbprint scanning being the favored option followed by retinal scanning (see Figure 18).
- Respondents see making transactions—such as paying bills or insurance premiums, or transferring funds—as the area where they would be willing to use biometrics (see Figure 19). However, there was hesitation about using biometrics for large transactions. Only 12% of those who prefer biometric based authentication were ready to use it to make transactions over $10,000.

Figure 18 – Preferred authentication modes



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

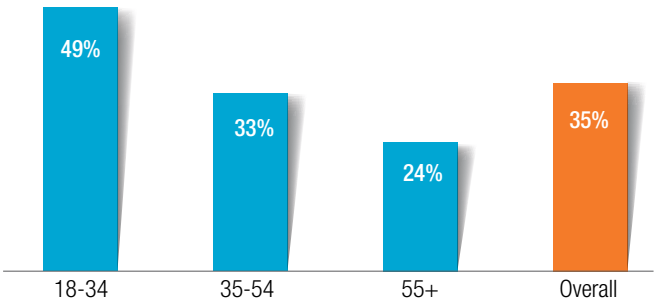
Figure 19 – Preferred application areas for biometric authentication



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

We did find that over a third (35%) of respondents are ready to pay for enhanced security. Of all age-groups, millennials expressed greater propensity to pay, signaling that they clearly value privacy the most and are willing to go the extra mile to guard it (see Figure 20). Banks and insurers have an opportunity here to differentiate their privacy and security offering, leveraging their investments in new security technologies.

Figure 20 – Millennials show higher willingness to pay for enhanced security than the rest



Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

To meet the different needs of consumers, organizations need to implement a three-tier security and privacy portfolio:

- **Bronze level:** Offers industry-standard security and privacy solutions at no additional cost with full compliance to all major regulations and data privacy standards such as General Data Protection Regulation , Payment Card Industry Data Security Standard (PCI DSS), and ISO 27001.
- **Silver level:** Offers advanced security and privacy services for clients requiring a higher level of data privacy and security standards. This level of service can be offered to consumers who would be willing to pay for enhanced security and/or are willing to share their personal data.
- **Gold level:** Offers premium security and privacy services (full anonymization in markets where it is not mandated by law, no sharing even if permitted by law, etc.) for a very limited amount of clients who are very sensitive to these issues.

As they introduce advanced authentication solutions, banks and insurers will also need to strike a balance between convenience and security. Inconvenience or delays in authentication are significant barriers to adoption[14]. Those banks and insurers who are able to implement 'easier to use and secured authentication techniques' will see more traction—and increased trust—from consumers.

Automate cybersecurity intelligence

Organizations will need to automate their security intelligence and make it more relevant, actionable, and real time. Automated intelligence built on advanced analytics platform is transforming the future of cybersecurity. Software vendors are also beginning to introduce tools that blend automation with cognitive approaches.

Moreover, automating security intelligence helps an organization's security operations center (SOC) to improve the effectiveness of security monitoring systems and reduce incidence response time[15].

Strengthen governance and security standards, from the top

Combating cyber risk requires more than just innovative technologies. Organizations must integrate business objectives with security and privacy priorities, managing digital risk across the enterprise (see "Why financial institutions must move towards industrialized 'Digital Security'"). To make this happen, boards need to get actively involved, particularly in insurance organizations, where less than half have a board that is actively engaged in cybersecurity matters. Boards must co-ordinate the approach with the entire executive management team—not just the CIO—and empower the Chief Privacy Officer (CPO) to bring security to the top of the strategic agenda. They need to be clear that management has a defined perspective on the impact of a cyber-incident on the business and the skills, resources, and approaches to minimize its likelihood. Boards also need to work closely with the management to foster a culture where privacy and security principles are ingrained and becomes a part of everyone's job.

In terms of governance, responsibilities need to be clearly demarcated, with distinct reporting lines between implementation teams and risk governance and management teams to ensure no conflict of interest:

- The implementation team is tasked with the technical and operational aspects of cybersecurity and data protection and act as the first line of defense inside the IT department and using outsourced security services
- The (digital) risk management team covers aspects such as maintaining policies and procedures, monitoring effectiveness of cybersecurity and data protection controls, and ensuring regulatory compliance and reporting. They can serve as the second line of defense closer to business lines
- Internal audit is required to regularly review the activities of the first and second line of defense to ensure that the controls in place are functioning accurately[16].

Regulatory focus on cyber issues is increasing – with examples including the EU-wide Network and Information Systems (NIS) directive on cybersecurity[17] and proposed new regulations in the US on cybersecurity practices for banks with assets greater than $50bn[18]. It is important, therefore, for financial institutions to continually review their risk management practices. They also need to consolidate their approach to demonstrating compliance. This includes unified controls frameworks (multi-standard) and Governance, Risk and Compliance tools to implement continuous controls monitoring.

Why financial institutions must move towards industrialized "Digital Security"

The evolving risk landscape, and the global nature of banking and insurance businesses, require a different approach – one that takes a more comprehensive view of digital risks. The traditional approach of information security, which relies more on technology and systems, must give away to a more business and data-centric approach called "Digital Security." Digital Security encompasses all cyber threats (intrusion, abuse, sabotage, loss, theft, leaks and denial of services) and impacts. It has a strong focus on reputation, people and operations and encompasses cybercrime and fraud management, (physical) security and information protection, privacy and safety, business continuity and reliability.

From a governance perspective, the Digital Security program must be managed at a senior level in co-ordination with local security platforms within business lines and IT departments. The objective should be to break down silos, managing risks consistently. The transformation to digital risk management will rely on an industrialized threats-vs.-solutions analysis and processes with global data protection and privacy policies and monitoring activities.

Ṣource: Pierre-Luc REFALO, Capgemini Cybersecurity Unit-Global Head of Strategic Consulting, La sécurité numérique de l'enterprise, 2013

CONCLUSION

Banks and Insurers have reaped a perception dividend on privacy and security issues that other industries have not enjoyed. However, this advantage is under threat as transparency increases and consumers become more aware of breaches that do occur. If organizations do not take proactive steps to enhance security and privacy, consumers will quickly realize that their high levels of trust are perhaps misplaced, with significant consequences for the sector. Banks and insurers should consolidate their position as the trusted custodians of consumer data. They need to reinforce their cybersecurity defense program with state-of-the art security intelligence and breach detection capabilities. This, however, must be coupled with the right data practices if security investments are to deliver upon their potential. With this integrated approach, banks and insurers can continue to earn their customers' trust and build a winning skillset in a world where the amount of data that flows between them will only increase.

Research methodology

Capgemini conducted two global surveys to understand consumer perceptions and preferences and to gauge the state of institutions' data privacy and cybersecurity measures:

- A survey of retail banking and insurance consumers
- A survey of senior data privacy and security executives from banks and insurers.

The survey answered the following key questions:

- How do consumers perceive the way banks and insurance firms are handling their personal data?
- Are there any gaps between consumer perceptions and organizations' actions on data privacy?
- Are consumers willing to trade privacy for more convenience?
- What are the types of data that consumers are willing to share and the convenience they are looking for in return?
- Are organizations set up to handle consumer data in a secure way?
- How ready are organizations to comply with General Data Protection Regulation?
- What steps can organizations take to strengthen consumer data privacy and security?

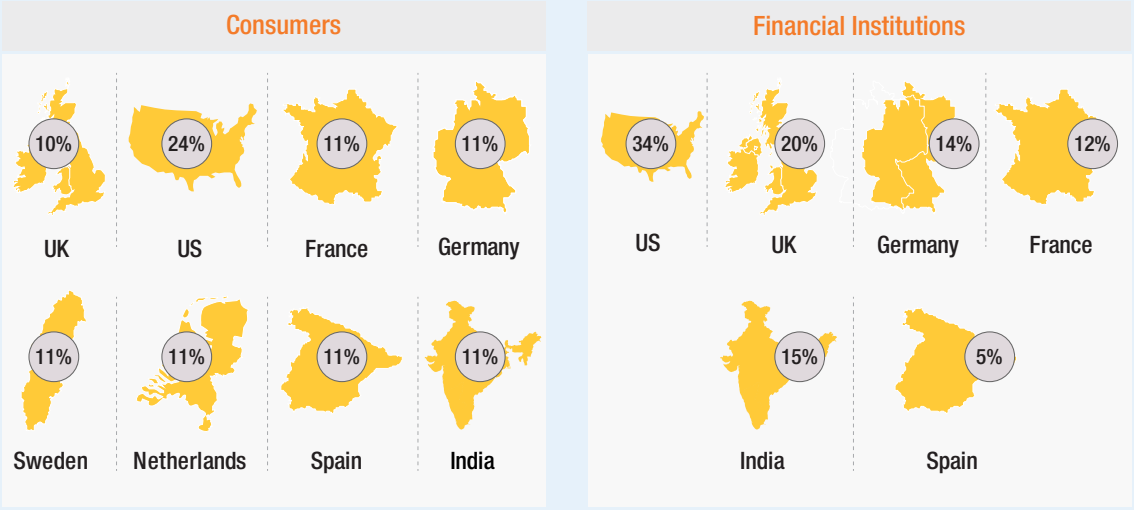
Consumer survey

We surveyed 7,600 consumers from eight countries across all age-groups (18 years to 55+ years) and income types to understand their data usage behavior, privacy preferences, data usage expectations and trust levels with handling of personal data. The online survey took place between September 2016 and October 2016.

Institutional survey

We surveyed 183 senior data privacy and security professionals from retail banks and insurance firms with 40% of organizations having global revenues of greater than $10 billion—to understand their data practices and cybersecurity strategies. The survey was conducted across six countries and three continents. The online survey took place in October 2016.

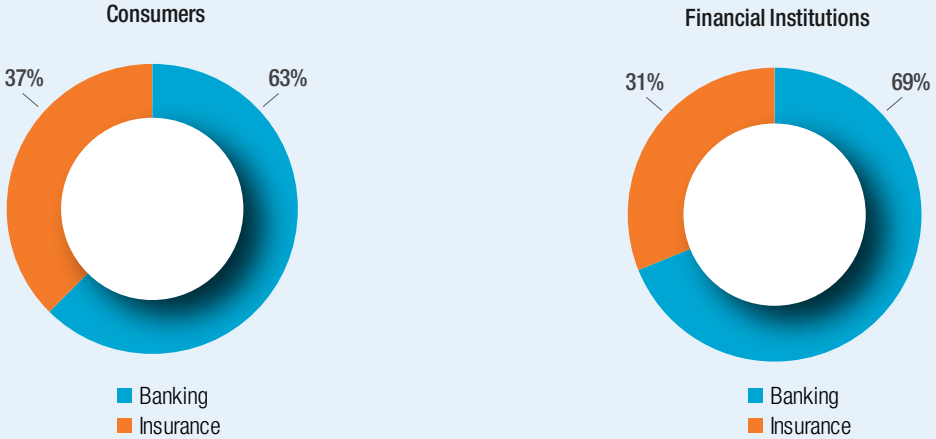
Split of respondents by geography



Survey of 7,600 consumers across 8 countries, on key data privacy and security-related issues. Both banking and Insurance consumers across all ages and income-types participated in the survey.

Survey of 183 senior data privacy and security professionals from banks and insurance firms with 40% of organizations having global revenues of greater than $10 billion. The survey was run across six countries and three continents.

Split of respondents by sector



References

1 American Banker, "Customer Data Is a Liability", January 2017
https://www.americanbanker.com/news/customer-data-is-a-liability
Financial Times, "Cyber attacks against UK financial industry on the rise — FCA", September, 2016
https://www.ft.com/content/66c95bc0-71b8-3adc-9e35-bef3e67b9292

2 Strength of Data Privacy policies – Assessment parameters

- **Governance and Design** assesses if data privacy has been embedded as a design guideline in the digital initiatives, level at which data policies are handled and if there are CXO level executives looking after data privacy.
- **Internal Access** relates to the policies on access to customer data by internal stakeholders and training and awareness programs.
- **Storage, retention and consent** identifies if the institutes have policies in place for storing as well as deleting customer data and if requisite consent from customers is taken for using their personal data.
- **Legal and compliance** checks if the data processing activities have a legal basis, if the privacy policies are frequently reviewed and also the state of readiness of the companies with respect to GDPR.
- **Audit and control** examines whether policies on access to data by external vendors are in place, how frequently these are reviewed and if the policies are audited and assessed.

Strength of Security framework – Assessment parameters

- **Governance** looks into the role of cybersecurity in the organization and its relative importance.
- **Security Budget** identifies if importance has been given to cybersecurity in the organization's budget.
- **Security Intelligence** assesses the organization's capabilities in handling various cyber threats.
- **Breach detection and management** looks at the organization's abilities regarding data breaches and their preparedness in the event of a data breach.

3 The Cyber Rescue Alliance Library Quotes
http://www.cyberrescue.co.uk/library/quotes

4 Verizon, "2016 Data Breach Investigations Report"
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

5 (a) the original purpose for collecting personal data is not over; (b) the data subject has given consent; (c) the processing is necessary for compliance with a legal obligation or to protect the vital interests of data subject; or (d) to protect the legitimate interests of data controller

6 ICO, "Notification of data security breaches to the Information Commissioner's Office (ICO)", July 2012
https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

7 The Privacy Advisor, "What will mandatory DPOs look like under the GDPR? Germany could tell you", June 2016
https://iapp.org/news/a/what-will-mandatory-dpos-look-like-under-the-gdpr-germany-could-tell-you/

8 European Digital Rights, "Key aspects of the proposed GDPR explained"
https://edri.org/files/GDPR-key-issues-explained.pdf

9 The Financial Brand, "Mobile Banking Usage to Double", August 2015
https://thefinancialbrand.com/53431/global-mobile-banking-usage-study/

10 Kaspersky, Security bulletin, 2015
https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

11 Capgemini Consulting, "Digital Transformation Review N' 6 - Crafting a Compelling Digital Customer Experience", August 2014
https://www.capgemini-consulting.com/digital-transformation-review-6

12 European Digital Rights, "Key aspects of the proposed GDPR explained"
https://edri.org/files/GDPR-key-issues-explained.pdf

13 The Cyber Rescue Alliance Library Quotes
http://www.cyberrescue.co.uk/library/quotes

14 Financial Times, "Banking biometrics: hacking into your account is easier than you think", November 2016
https://www.ft.com/content/959b64fe-9f66-11e6-891e-abe238dee8e2

15 BetaNews, "The 'age of automation' can benefit the security landscape", November 2016
http://betanews.com/2016/11/30/security-age-of-automation/

16 ISACA, "The Three Lines of Defence Related to Risk Governance", 2011
http://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Three-Lines-of-Defence-Related-to-Risk-Governance.aspx

17 Financier Worldwide, "Europe's new cyber security directive", March 2016
https://www.financierworldwide.com/europes-new-cyber-security-directive/

18 CNBC, "Regulators order banks to brace for cyber attacks", October 2016
http://www.cnbc.com/2016/10/19/regulators-order-banks-to-brace-for-cyberattacks.html

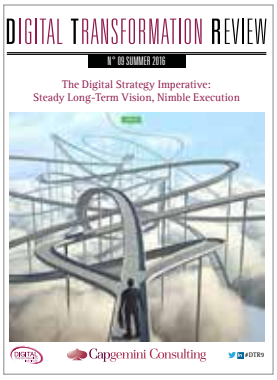
Discover more about our recent research on digital transformation

Stewarding Data: Why FS Firms need a Chief Data Officer

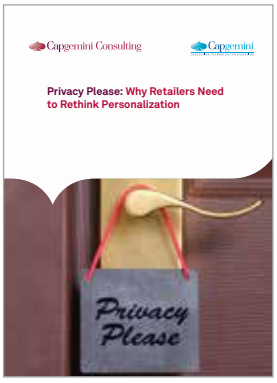
Fixing the Insurance Industry: How Big Data can Transform Customer Satisfaction

Smart Contracts in Financial Services: Getting from Hype to Reality

Big Data Alchemy: How can Banks Maximize the Value of their Customer



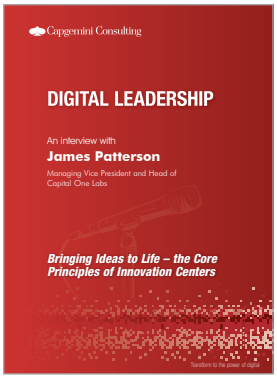
Digital Transformation Review 9: The Digital Strategy Imperative



Privacy please: Why Retailers Need to Rethink Personalization

Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT

Digital leadership : Visa: The FinTech Giant Leading Digital's Platform Revolution



Digital leadership : Bringing Ideas to Life: the Core Principles of Innovation Centers

About the Authors

Maliha Rashid
Principal, Cybersecurity Leader, Capgemini Consulting France
maliha.rashid@capgemini.com

Maliha leads the cybersecurity practice for Capgemini Consulting in France. She has 14 years of experience in cybersecurity and works with major banks on their cybersecurity programs.

Zhiwei Jiang
Global Head of Financial Services Insights & Data, Capgemini
zhiwei.jiang@capgemini.com

Zhiwei is the Global head of financial services insights and data at Capgemini. He is based in London.

Pierre-Luc REFALO
Director, Global Head of Strategic Cybersecurity Consulting, Capgemini.
pierre-luc.refalo@sogeti.com

Pierre-Luc has more than 25 years in info & cybersecurity consulting business development. He is an author and speaker in international events.

Jerome Buvat
Head, Digital Transformation Institute
jerome.buvat@capgemini.com
@jeromebuvat

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

Subrahmanyam KVJ
Senior Manager, Digital Transformation Institute
subrahmanyam.kvj@capgemini.com
@Sub8u

Subrahmanyam is a senior manager at the Digital Transformation Institute. He loves exploring the impact of technology on business and consumer behavior across industries in a world being eaten by software.

Kunal Kar
Manager, Digital Transformation Institute
kunal.kar@capgemini.com

Kunal is a manager at Capgemini's Digital Transformation Institute. He tracks the impact of digital technologies on the financial sector and helps clients on their digital transformation journey.

Digital Transformation Institute

dti.in@capgemini.com

The Digital Transformation 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 and India.

The authors would like to especially thank Ramya Krishna Puttur from Capgemini Consulting's Digital Transformation Institute for her contributions to this report.

The authors would also like to thank Apoorva Chandna from Capgemini's Digital Transformation Institute; Nathalie Laneret, Capgemini Group Data Protection Officer; Ron Tolido, Global CTO, Insights & Data, Capgemini; Ashvin Parmar, Harbir Brar, Nilesh Vaidya, Kevin Hart, Ian Campos from Capgemini North America; Clare Argent, Srikant Kanthadai, Sandeep Kumar, Jelger Groenland, Ralf Teschner from Capgemini UK; Rutberg Klas from Capgemini Consulting Sweden; Erik Hoorweg, Albert Holl, Andre Walter, Melle van den Berg from Capgemini Consulting Netherlands; Isabelle Budor, Stanislas De Roys, Jean-Charles Croiger from Capgemini Consulting France; and Markus Filkorn from Capgemini Consulting Germany for their contribution to this research

For more information, please contact:

Global

Zhiwei Jiang
zhiwei.jiang@capgemini.com

Sri Kanthadai
srikant.kanthadai@capgemini.com

Ron Tolido
ron.tolido@capgemini.com

Jean Coumaros
jean.coumaros@capgemini.com

Mike Turner
mike.a.turner@capgemini.com

Harbir Brar
harbir.brar@capgemini.com

Nilesh Vaidya
nilesh.vaidya@capgemini.com

Oswin Deally
oswin.deally@capgemini.com

France
Stanislas de Roys
stanislas.deroys@capgemini.com

UK
Kristofer le Sage de Fontenay
kristofer.le-sage-de-fontenay@capgemini.com

Belgium
Robert van der Eijk
robert.van.der.eijk@capgemini.com

Netherlands
Tamara Monzon
tamara.monzon@capgemini.com

US
Alvi Abuaf
alvi.abuaf@capgemini.com

Sweden and Finland
Johan Bergstrom
johan.bergstrom@capgemini.com

Germany, Austria and Switzerland
Christian Kroll
christian.kroll@capgemini.com

Tamara Monzon
tamara.monzon@capgemini.com

Spain
Christophe Mario
christophe.mario@capgemini.com

David Brogeras
david.brogeras@capgemini.com

China
Kevin Zhu
kevin.zhu@capgemini.com

Norway
Jon Waalen
jon.waalen@capgemini.com

Hong Kong and Singapore
Frederic Abecassis
frederic.abecassis@capgemini.com

Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, the global team of over 3,000 talented individuals work with leading companies and governments to master Digital Transformation, drawing on their understanding of the digital economy and leadership in business transformation and organizational change.

Find out more at: www.capgemini-consulting.com

Rightshore® is a trademark belonging to Capgemini

About Capgemini and the Collaborative Business Experience

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business ExperienceTM, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at www.capgemini.com.