FROST & SULLIVAN

ca technologies

The Global State of Online Digital Trust

A Frost & Sullivan White Paper

COMMISSIONED BY CA TECHNOLOGIES

THE IMPORTANCE OF ONLINE TRUST IN THE DIGITAL ERA

Amidst a continuous stream of headlines about major data breaches in enterprise and government agencies, the degree to which consumers have placed their trust in organizations to protect their personally identifiable information (PII) online has never been more relevant. In 2017 alone, the number of confirmed data breaches globally was staggering.[1] Equifax, Reliance Jio, Netshoes, Deloitte, Uber, CEX, Jins, and Ticketmaster comprise just a sample of well-known brands that were involved in data breaches. Meanwhile, in early 2018 it was revealed that Cambridge Analytica was not only exploiting Facebook user data to manipulate millions, it was openly boasting[2] about interfering in multiple elections globally.

Against this backdrop, it is crucial for business leaders to understand public sentiment concerning sharing their information online, as it has **tangible consequences for their bottom line**. And the consensus among consumers is clear: in a survey conducted by Frost & Sullivan and CA Technologies, 78% of consumers responded that it is very *important* or *crucial* that their PII be protected online. Virtually no respondents indicate that protecting PII is not important. Furthermore, 86% indicate that a high level of data protection is a priority when choosing online services.

78% of consumers responded that it is very **important** or **crucial** that their PII be protected online.

Consumer trust in online services drives usage patterns: **when a data breach is reported, 48% stop using that service**. A well-known adage in the information security profession about data breaches is that for organizations it is not a question of *if* a breach will occur, but *when*. Half (48%) of organizations surveyed report having been involved in a publicly disclosed data breach, and nearly all found that the breach had a long-term negative impact to their revenues and to consumer trust. Half of those whose organizations that have been breached report a strong long-term negative impact not only on consumer trust (50%), but also on their business results (47%).

In light of this, understanding what drives online digital trust is of paramount importance to business leaders. The survey conducted for this study examines this issue from the perspective of consumers, business executives, and information security professionals. The results reveal an extraordinary disconnect between the experiences of consumers and the perceptions of organizations who provide online services.

The precarious nature of digital trust is illustrated by the decline of consumer trust in organizations over the past two years—**only 38% indicate that their trust has *increased*, contrasted against the perceptions of business leaders, 84% of whom believe that consumers trust them more now than they did two years ago.** It is apparent that organizations are **dangerously out of touch** with their customers.

The digital trust perception gap, and other findings in this ground-breaking study, highlight the need for business leaders to understand how much consumers trust organizations, what drives digital trust, and the business impact of losing that trust.

---

1 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

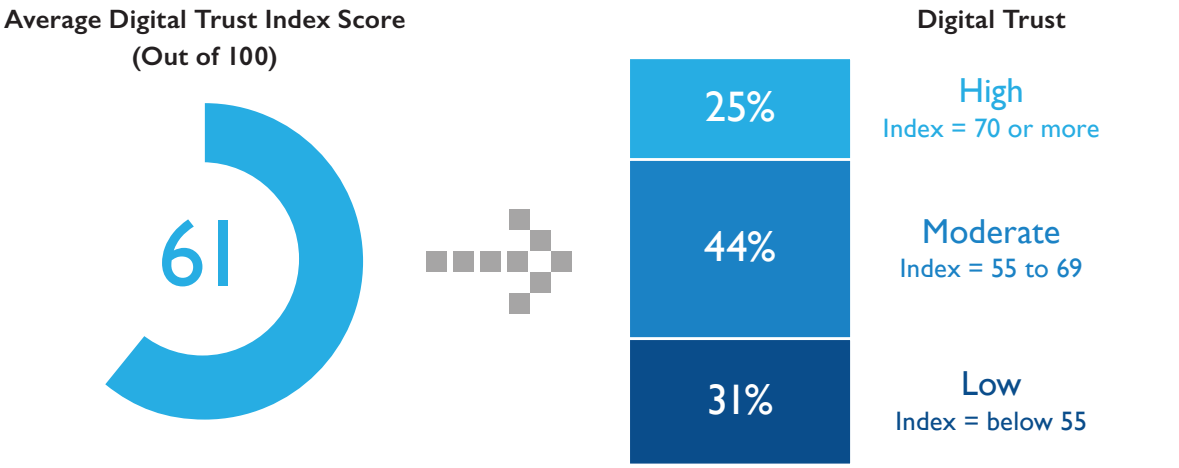
2 https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections

THE DIGITAL TRUST INDEX

Quantifying an issue such as digital trust can be challenging for business leaders, so CA Technologies and Frost & Sullivan developed a series of metrics for different facets of consumer digital trust to create The Digital Trust Index. Some metrics include whether consumers believe organizations take appropriate precautions to protect PII, as well as consumer willingness to share their PII online. By aggregating multiple digital trust variables, it was possible to segment consumers into three categories: those with high levels of digital trust, those with moderate levels, and those with low levels of trust. Additionally, the Index assigned a score between 1 and 100 to quantify the average level of digital trust among consumers. The average digital trust score in 2018 is 61 out of a possible 100. One way to contextualize the score is to compare it to academic settings in many parts of the world where 61 is barely a satisfactory score, with substantial room for improvement.

The average digital trust score in 2018 is 61 out of a possible 100.

Exhibit 1: The Consumer Digital Trust Index



Source: Frost & Sullivan, N = 990

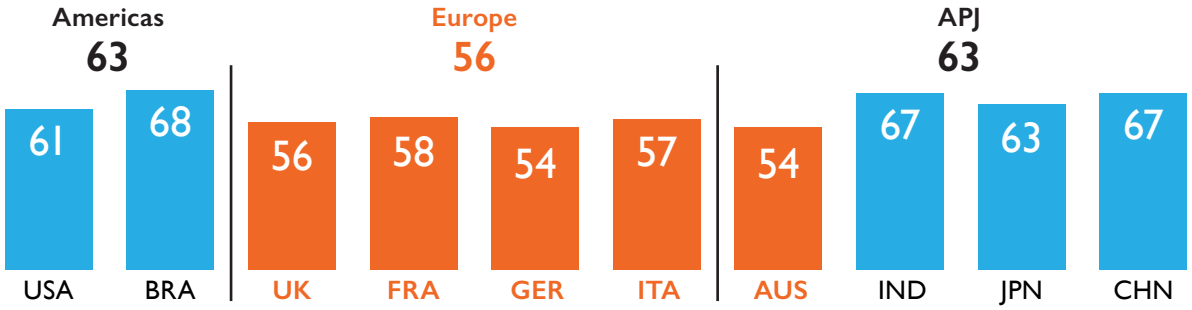
Examining the consumer segments more closely reveals that nearly half, or 44%, of consumers occupy the moderate digital trust range, with a score between 55 and 69. Thirty one percent were found to have low levels of digital trust, while the smallest number of consumers, 25%, falls in the upper tier of digital trust.

Overall, only half of consumers (49%) are willing to provide their personal data in exchange for digital services, but 54% distrust organizations enough to believe that they will sell their personal data to other companies.

Given the near-weekly news of new data breaches, an average score of 61 out of 100 in digital trust seems reasonable, because it reflects an underlying belief in the ability of organizations to protect data, but is overlaid with deep scepticism about the degree to which they are taking the proactive steps necessary to succeed.

There are geographic patterns in global digital trust. The Index shows a significantly lower degree of trust in Europe and Australia compared to the rest of the world.

Exhibit 2: The Consumer Digital Trust Index by Region



Source: Frost & Sullivan, N = 990

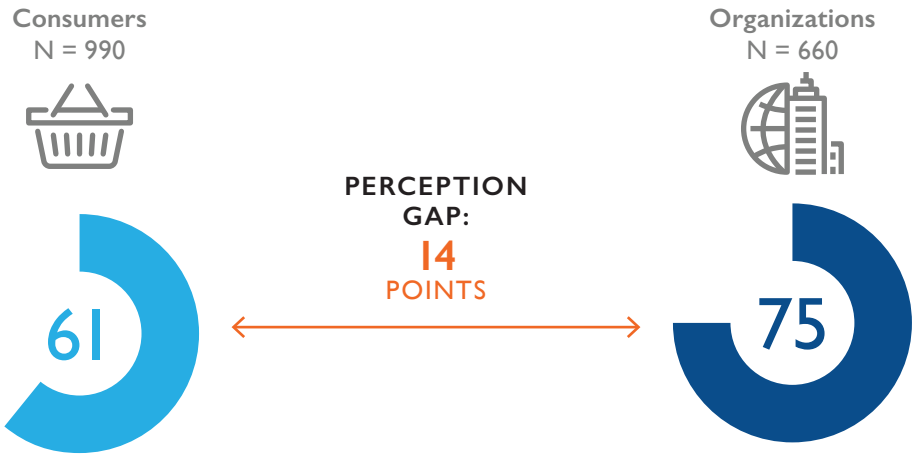
Lower trust levels in Europe can be attributed to the legacies of the last World War and the fall of communism in Europe. During both eras, privacy was superseded by many governments that used PII to institutionalize discrimination and human rights abuses. The result of that shared history has been the creation of laws within the European Union that uphold individual privacy as a basic human right. In the digital era, those rights are increasingly perceived as under threat by the organizations that consumers do business with online. The causes for this perception are varied, and include trends such as data retention, the creation of consumer profiles, and a notable increase in the volume and severity of data breaches.

In the APJ region, Australia is distinct due in large part to its European heritage which continues to be a strong cultural influence, as opposed to India, Japan, and China. Australia's European heritage has not only resulted in strong and on-going linkages to Europe, but has also translated into a European-style perspective that influences modern Australia and its concerns about PII, privacy, and digital trust.

The Digital Trust Divide

Global organizations, however, see digital trust differently. When asked a similar set of questions regarding their perceptions of whether consumers trust them, an altogether different picture emerges. **On average, organizations scored 75 out of 100** when estimating the degree to which consumers trust their organizations to handle their personal data appropriately.

Exhibit 3: The Consumer Digital Trust Index Compared to the Perceptions of Organizations

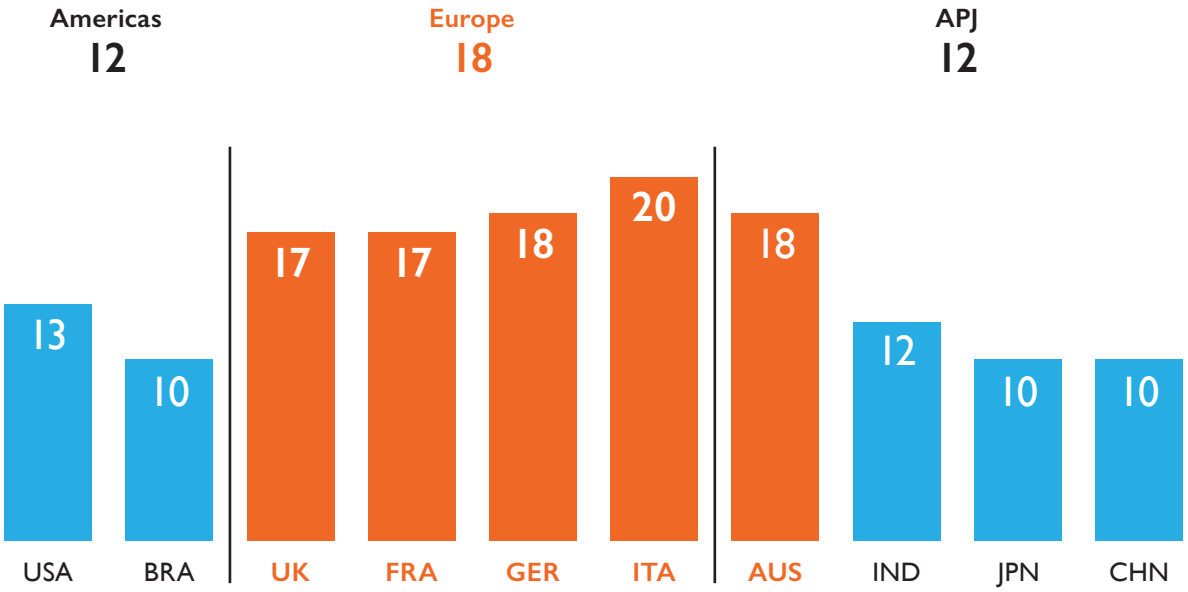


Source: Frost & Sullivan

There is a 14 point perception gap in how organizations perceive customer's trust in their ability to handle personal data appropriately compared to the consumer's level of trust in their ability to manage this process. Simply put, business leaders overestimate consumer trust in their organizations. Nowhere is this trend more noteworthy than in Europe and Australia.

Simply put, business leaders overestimate consumer trust in their organizations.

Exhibit 4: The Consumer Digital Trust Index Perception Gap of Organizations by Country and Region



Source: Frost & Sullivan, N = 990

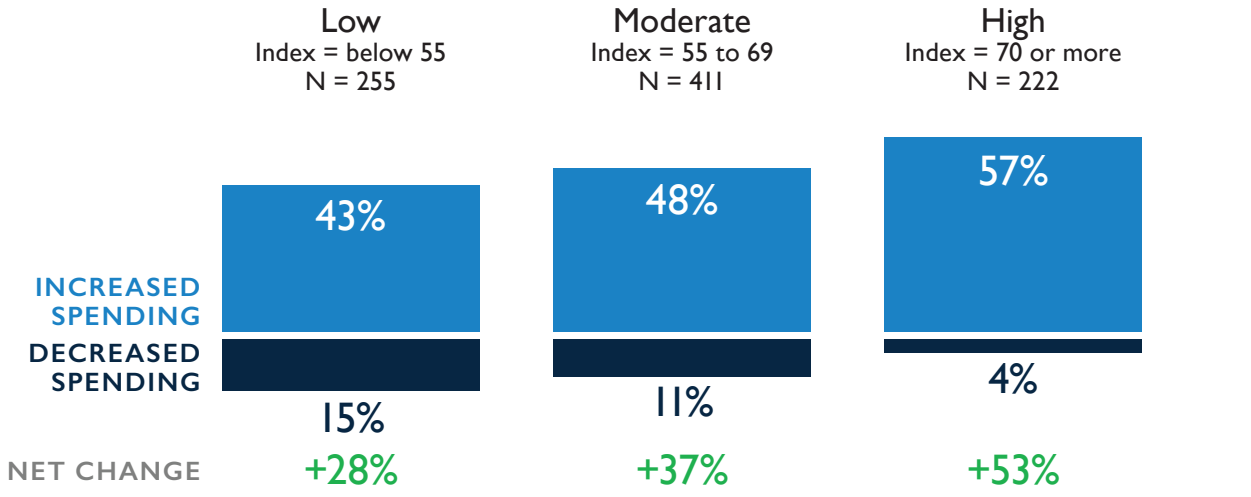
On average, European business leaders are most likely to overestimate the degree to which consumers trust online services, and generally the overarching global trend is to overestimate levels of consumer digital trust.

The global perception gap is likely connected to numerous recent data breaches and on-going data privacy scandals, and to the declining state of consumer willingness to share their personal information online—**22% indicate that their trust has decreased in the past two years, while the vast majority of organizations believe that trust has increased over that same timespan**. To reconcile that perception gap, organizations must do far more than simply acknowledge the importance of trust. They must undertake proactive efforts to understand the importance of trust among consumers as well as its impact on business revenues.

CONSUMERS CARE ABOUT TRUST

Organizations must understand that trust plays an important role in determining which online services consumers use and where they choose to purchase goods and services online. There is a direct correlation between where consumers fall on the Digital Trust Index and their likelihood to spend online, which has clear implications for every online business model around the world.

Exhibit 5: Change in Online Spending Habits Over the Last 12 Months by Level of Digital Trust

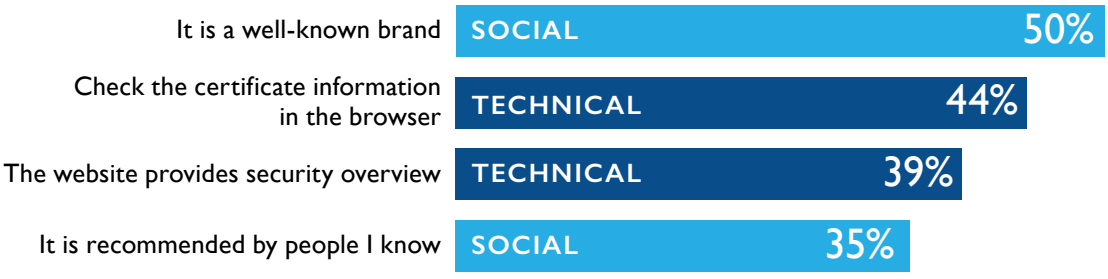


Source: Frost & Sullivan

While the trend across all consumers shows an increase in online spending over the past 12 months, those with the highest levels of digital trust increased their net spending online significantly more compared to those with the lowest. In Germany, where 42% of consumers fall into the low digital trust segment, 22% with low trust report spending less online in the past 12 months—the most significant decrease in the Western world. It is therefore crucial for organizations to understand what drives trust, and how consumers determine which companies have the strongest data protection measures that can generate higher digital trust.

Both social and technical factors influence how consumers determine whether an online service provides strong data protection. Among the factors driving digital trust, the top contributors are brand image, security certificates, an explicit security overview, and recommendations from personal connections.

Exhibit 6: Factors Driving Consumer's Perception of Data Protection Measures



Source: Frost & Sullivan, N = 990

Brand recognition, perhaps predictably, is the most widely cited factor that drives consumer belief in the ability of an organization to protect their data, however many users also monitor the service's security certificate information and look for a comprehensive security overview. Personal recommendations, or word of mouth, round out the top drivers of perceived data security. On average, social factors are cited by 43% of consumers, and technical factors are cited by 42%, rendering the two equally important for organizations to consider. Among those with low digital trust, social factors are cited by just 34%, while technical factors

are cited by 40%. Among those with high digital trust, social factors assume greater importance than among those with low trust, with 47% citing social factors.

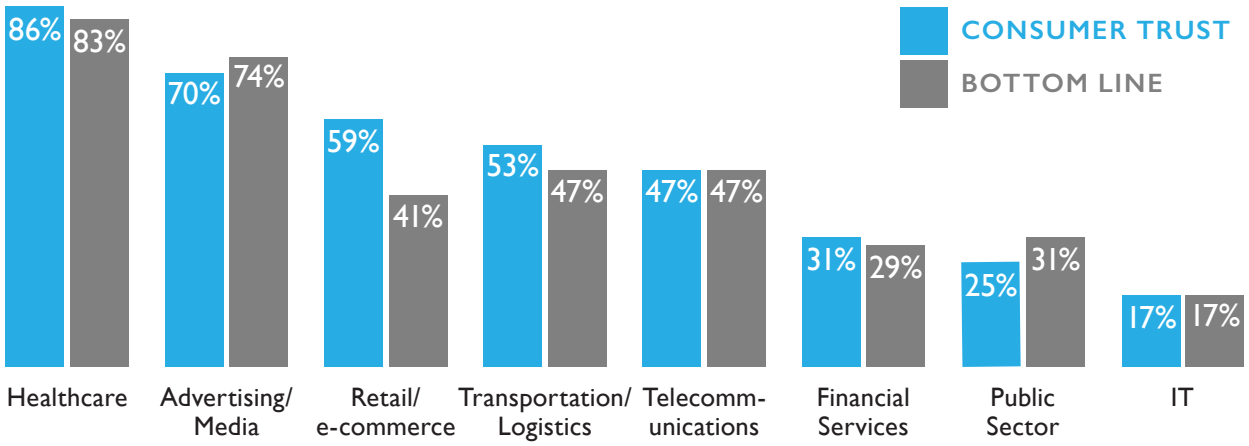
Higher digital trust is directly correlated with increased spending online, and a relatively small number of factors account for the public's perception of the strength of an organization's data protection. But business leaders must be conscious not only of the positive effects of gaining digital trust, but also of the negative impact of losing it.

On average, social factors are cited by 43% of consumers, and technical factors are cited by 42%, rendering the two equally important for organizations to consider.

LOSING DIGITAL TRUST: A TANGIBLE BUSINESS IMPACT

The degree to which companies have experienced a strong negative impact following a data breach is significantly influenced by the industry in which they operate. Healthcare organizations are by far the most likely to report strong negative impacts on consumer trust and their bottom line as the result of a data breach.

Exhibit 7: STRONG Negative Impact as a Result of a Data Breach, by Industry



Source: Frost & Sullivan, (N = 208)

It is not surprising that healthcare organizations suffer greatly in the event of a breach; however, perhaps the most interesting finding is the relatively small number financial services firms that indicate they have suffered a strong negative impact due to a data breach. Financial services firms may have higher immunity to the negative impacts of data breaches because of their swift reactions to incidents, including the cancellation and reissue of credit cards, forced password resets, proactive fraud prevention departments, and security awareness campaigns directed towards customers.

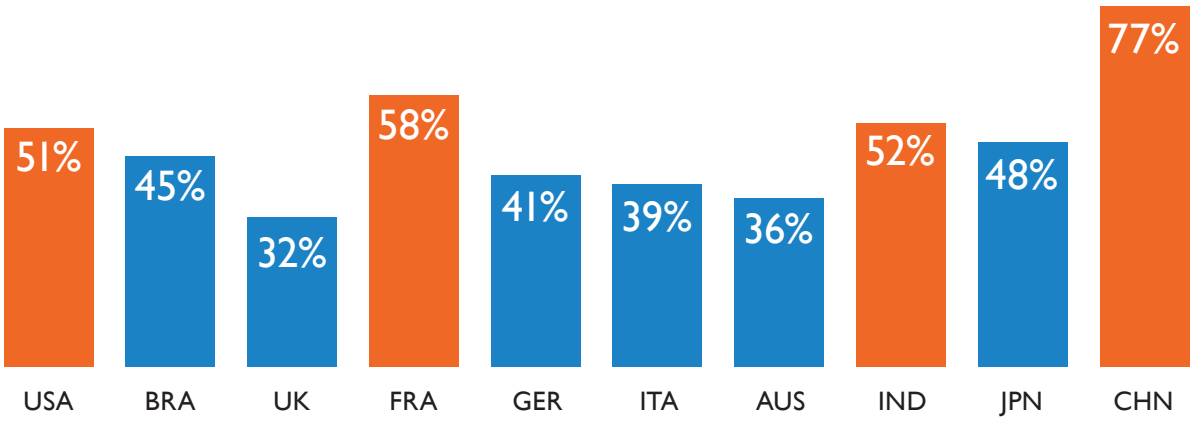
Consumers are weary of organizations that been involved in data breaches. Moreover, when personal data is exfiltrated in a data breach, half (48%) of consumers also view the incident as a breach of their trust and stop using the online service that lost control of their data.

CXOs and their executive teams can no longer tell information security professionals that strong security tools, controls, processes, and training to protect sensitive PII are too costly and a hindrance to business. The data shows that organizations that do not take proactive measures to properly protect PII can expect long-term negative impacts to revenues, as half of all consumers have demonstrated their willingness to shift their business to a competitor after a breach.

Although the outcome of a publicly disclosed breach is nearly always negative, consumers in some countries are more forgiving of breaches than others.

Moreover, when personal data is exfiltrated in a data breach, half (48%) of consumers also view the incident as a breach of their trust and stop using the online service that lost control of their data.

Exhibit 8: STOPPED Using an Online Service After Breach Disclosure, by Country



Source: Frost & Sullivan, (N = 402)

In the United States, France, and India, more than half of those who at one point used a service stopped after news of a data breach surfaced. Most notable, however, is the number of Chinese consumers who say the same: nearly 8 in 10 (77%) indicate that they stopped using a service after hearing news of a data breach. Paradoxically, China is where the growth in digital trust is highest, with a net growth in trust in organizations of 67% over the past two years. Chinese consumers are therefore unique in the world: their digital trust growth outpaces other nations, yet they also are the most unforgiving in the event of a data breach.

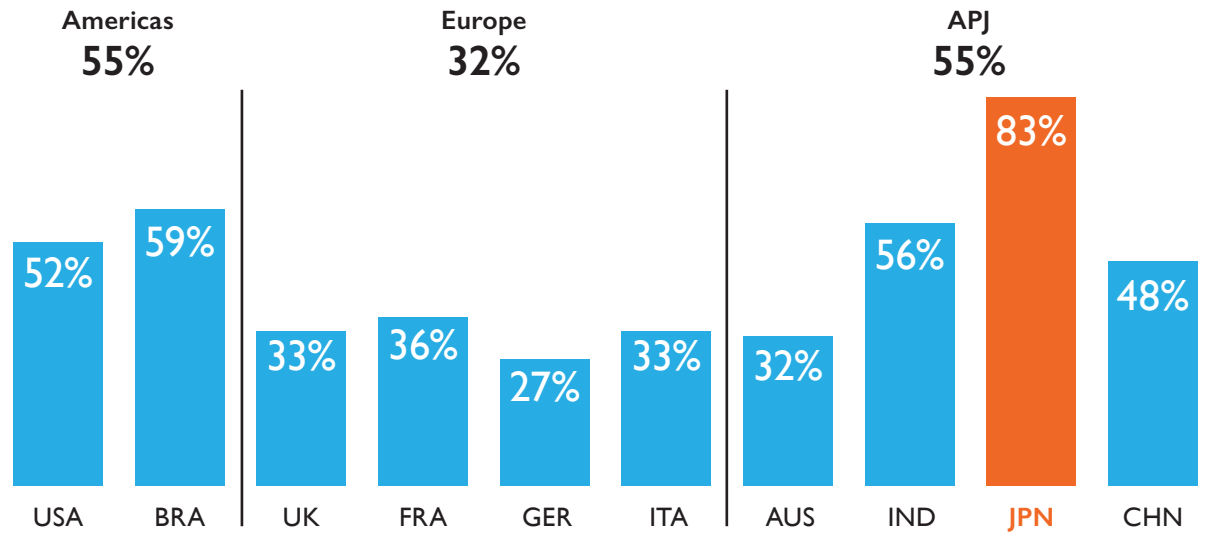
Data breaches, while clearly significant, account for only one of the ways organizations can contribute to the erosion of consumer trust. In the wake of the Facebook/Cambridge Analytica scandal, the public is increasingly aware not just of breaches, but of how their data is shared and what it is used for even when it is 'secure.'

The Monetization of Personally Identifiable Information

Sharing and monetizing PII is a contentious topic, despite widespread reporting[3] on its prevalence. Data brokers often are not effectively securing consumer data,[4] and some have leaked data on millions of consumers.[5] Of the many issues associated with the monetization of PII, perhaps the most commonly referenced problem is a lack of awareness among consumers whose information is for sale. Globally, 46% of consumers do not believe or are unsure if the services they use sell their PII. Predictably, this number increases among consumers with higher levels of digital trust—73% of those who are ranked High on the Digital Trust Index do not believe their PII is shared or sold.

Consumers around the world have varying degrees of belief in the extent to which their PII is sold by online services that they use, with stark regional differences.

Exhibit 9: DO NOT Believe or are Unsure If Organizations Sell Personal Data, by Country and Region



Source: Frost & Sullivan, (N = 990)

In each region save for Europe, the majority of consumers do not believe their PII is being bought or sold. In Japan, that number jumps to more than four in five consumers. The responses of Japanese consumers are the result of an amended data protection law—the Personal Information Protection Act (PIPA)—that went into effect in May 30, 2017.[6] The PIPA is a ground-breaking data privacy law which requires explicit consent from a consumer before PII can be obtained, and it allows the Japanese data protection authority (Personal Information Protection Commission) to oversee who provides and who receives PII to prevent its misuse.[7] The result of the regulation has been an increase in confidence amongst Japanese consumers that their PII is not for sale without their knowledge and consent.

3 https://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/

4 https://techcrunch.com/2018/06/19/verizon-stops-selling-customer-location-to-two-data-brokers-after-one-is-caught-leaking-it/

5 https://www.wired.com/story/exactis-database-leak-340-million-records/

6 https://www.ppc.go.jp/en/legal/

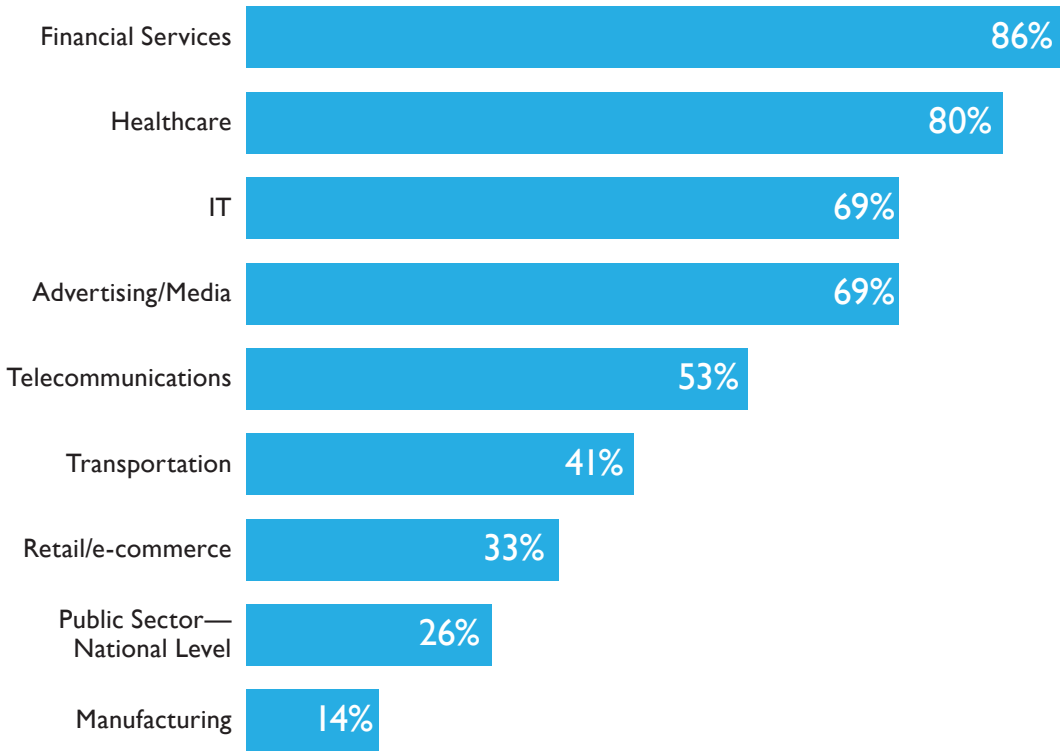
7 https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf

Low Awareness; Common Business Practice

The lack of consumer awareness of the potential sale of PII contrasts sharply with the reality of the business world: 43% of business leaders indicate that they sell personally identifiable customer data to other organizations. This revelation belies the carefully crafted industry rhetoric around selling consumer data,[8] with nearly half of business executives admitting that they do. Those who admit to selling PII point to language couched in their terms and conditions (T&C) policies, to which consumers must consent to use the service. These types of T&C policies are under scrutiny in the European Union because they could be interpreted as forced consent[9] by the General Data Protection Regulation (GDPR). Often, even when consumers choose to pay a fee to use a service, many organizations retain the right to repurpose customer data for sales, marketing, or other revenue enhancement initiatives.

43% of business leaders indicate that they sell personally identifiable customer data to other organizations.

Exhibit 10: Business Executives Cite Terms of Service Allow Sharing or Selling of Data, by Industry



Source: Frost & Sullivan, (N = 324)

The data also shows that **only half of consumers (49%) indicate that organizations provide them with an easy to understand data protection policy framework, while 85% of organizations indicate that they provide this information in a clear, easy to understand format**. This is not particularly surprising, as

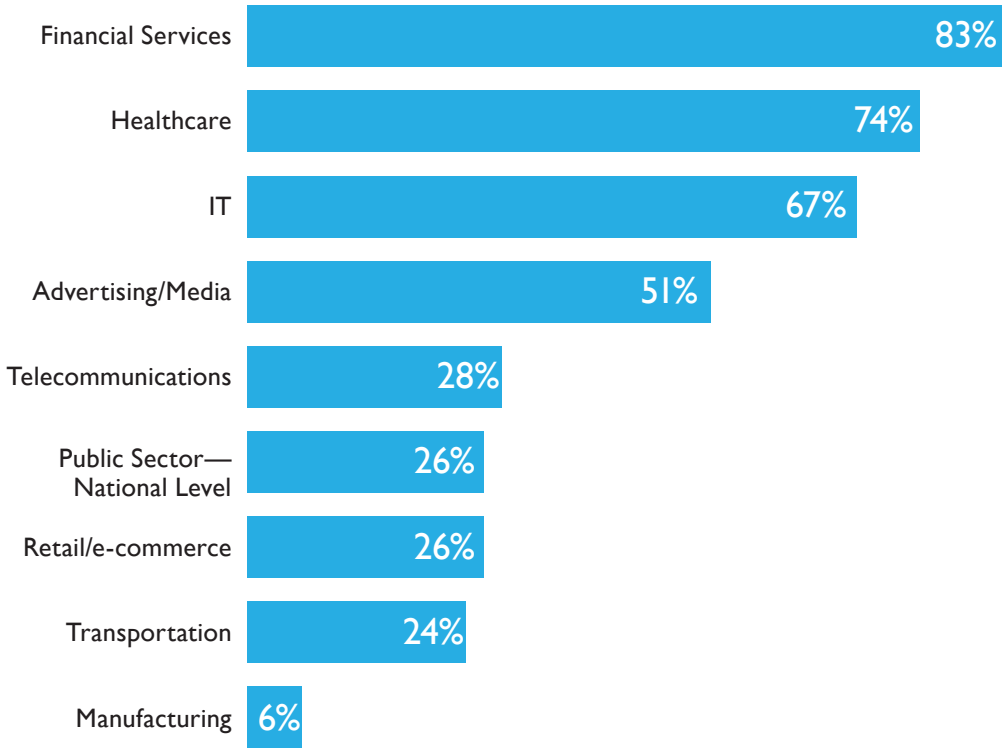
8 https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought

9 https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

previous Frost & Sullivan research discovered that T&C policies written by lawyers are lengthy and potentially confusing, even for university educated consumers. Further, many vendors interviewed by Frost & Sullivan candidly admitted that consumers have no idea what they were agreeing to in T&C policies. That could begin to change as a result of the GDPR in the European Union (EU) that requires clear, concise, plain language that is easy to understand, and easily accessible. Thus the policies of every company doing business in the EU, regardless of the location of their corporate headquarters, will have to comply to avoid fines of €20 million or 4% of global annual revenue, whichever is greater.[10]

The extent to which PII is sold to other organizations differs dramatically in different industries. A large proportion of financial services organizations, for example, sell PII, whereas in the manufacturing sector the practice is virtually non-existent.

Exhibit 11: Business Executives State Their Organization Sells Personally Identifiable Information, by Industry



Source: Frost & Sullivan, (N = 324)

The sale of PII is most common in financial services, healthcare, IT, and advertising/media. Healthcare and financial services are particularly noteworthy in their sale of PII, **as both hold extremely sensitive customer data**.

In the financial services industry, sharing or selling consumer data is a common practice because it enables potential lenders to assess the risk of doing business with an individual.[11] Unfortunately the collection and sale of this type of data in the financial services community makes companies with this type of highly sensitive

10 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

11 https://www.inc.com/associated-press/equifax-data-money.html

information targets by cyber adversaries. This was dramatically highlighted in 2017 following the Equifax data breach that impacted approximately 146.6 million Americans, 861,000 U.K citizens, and 8,000 Canadians.[12]

The sale of data in the healthcare industry is equally concerning due to the sensitive nature of the information. In most nations, healthcare data is de-identified before it is sold to third parties, with the intent of protecting privacy.[13] On the surface de-identification seems sufficient to protect individual privacy, but the reality is that data from fitness devices, search engines, and predictive analytics technologies widely available today have the ability to re-identify medical data to an individual.[14] The ability to re-identify medical data was proven by the University of Melbourne, Australia with a dataset of 2.9 million people.[15]

With the difficulty of de-identification and the growing popularity of new services, such as direct-to-consumer genetic testing, new privacy challenges such as unintentionally revealing data about relatives are arising that few consumers thought were possible.[16] Unfortunately the number of companies that privately purchase healthcare data make it virtually impossible for an individual to regain control of their DNA "fingerprint" after they have released a sample to a third party.[17] Adding to the privacy challenge, data aggregators are selling PII back to private insurance providers that could be used by actuaries to determine healthcare insurance premiums or if a policy can be sold.[18]

Information Security Personnel and the Monetization of PII

Nearly as concerning as the lack of awareness among consumers is the lack of understanding of how PII is used by individuals within the same organization. While 43% of business executives say they sell PII, only 15% of information security professionals report that their organization sells PII to other organizations—a 28 percentage point gap. The dissonance between business executives and information security professionals isn't surprising. That's because information security professionals are not always involved in business decisions regarding the monetization of company data. However, it raises an important question—are information security professionals positioned to really understand what is happening in the organization?

While 43% of business executives say they sell PII, information security professionals are generally unaware of the practice.

The answer to that question depends largely on the security maturity of an organization. The more mature an organization is, the more likely it is to have implemented security tools, processes, and training across the entire organization with formal guidelines.[19] Since the majority of organizations do not adhere to all security best practices, it's not surprising that information security professionals are frequently not consulted regarding

12 https://www.bankinfosecurity.com/equifax-us-breach-victim-tally-stands-at-1466-million-a-10985

13 https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

14 https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns

15 https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy

16 https://www.nytimes.com/2018/04/26/us/golden-state-killer.html

17 https://www.bloomberg.com/news/articles/2018-06-15/deleting-your-online-dna-data-is-brutally-difficult

18 https://www.nytimes.com/2014/06/29/technology/when-a-health-plan-knows-how-you-shop.html

19 https://www.secureworks.co.uk/resources/wp-security-preparation-are-uk-enterprises-doing-enough

decisions of how data, and which data leaves the organization. Involving information security professionals in these decisions however is critical to the business since they frequently know more about security, privacy, and data breach regulations than line of business executives. In fact, the exclusion of information security professionals from discussions around monetization of consumer data could inadvertently expose organizations to fines associated with data privacy laws.

The lack of awareness surrounding the sale of consumer data highlights a business-critical fissure between company executives and information security professionals.

The lack of awareness surrounding the sale of consumer data highlights a business-critical fissure between company executives and information security professionals. The opaque practice of selling consumer data will not boost consumer trust in organizations, and trust translates concretely into bottom line results. In light of the revelation that nearly half of organizations sell customer data, replete with PII, organizations cannot increase consumer trust by ensuring that their data protection policies are robust and transparent; even when data is well protected by one organization, when it is sold, the purchasing organization may not have similarly robust data protection capabilities in place.[20] Thus, a better way to enhance the digital trust of consumers is with a data protection and privacy policy that follows best practice guidelines developed in parts of the world with stringent data privacy laws.

ORGANIZATIONS MUST DO MORE TO PROTECT CUSTOMER DATA

When market forces are resistant to self-governance, government steps in to establish common rules in the form of regulations. In 2003 one of the largest economies in the world, the state of California,[21] passed Senate Bill (SB) 1386, a ground-breaking data breach notification law that is widely credited as the beginning of the era of publicly disclosed data breaches.[22] To enhance the law, California passed Assembly Bill (AB) 1950 in 2004 to legally impose duty of care responsibilities on organizations that keep consumer PII[23] and oblige them to follow a standard of reasonable security while collecting, storing, and processing PII.

California's AB 1950 was also ground-breaking because it established the concept of extended duty of care for securing data. This obligated all organizations that disclose consumer PII to non-affiliated third parties to require by contract that the third party implement and maintain reasonable security procedures and practices to protect PII from unauthorized access, destruction, use, modification, or disclosure. The concept of extended duty of care for consumer PII has become the gold standard for modern government regulations. The most recent of the modern regulations to hold the primary organization (the data controller) and unaffiliated third parties responsible for data breaches is the European Union's GDPR. Compliance with the law requires a contract between the companies that states the third party is in compliance with GDPR and

20 https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/

21 https://www.businessinsider.de/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5

22 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200120020SB1386

23 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200320040AB1950

in some instances third parties are required to submit to security audits to protect the data controller from potential liability.

Executives Need to Understand Organizational Shortcomings to Improve

The goal of a more robust and transparent set of data protection and privacy policies might be difficult to achieve if organizations do not become more self-aware. The overwhelming majority of organizations (93%) claim that they differentiate from competitors by providing better consumer data privacy than others. In addition, 90% claim that they are very good or excellent at protecting consumer data.

However, this degree of confidence in data protection protocols among organizations may be unwarranted. More than half (52%) of organizations who claim to have excellent data protection indicate that they have been involved in a data breach, and 47% of those who strongly differentiate from their competition based on their data protection have also been involved in a data breach.

Furthermore, there is a misconception among organizations regarding the ease with which consumers believe they can protect their data online. **Only 35% of consumers indicate that it is easy for them to protect their data online, while 65% of organizations believe it is easy for customers to protect the data they provide online**. The enormous gap between consumer reality and the unrealistic perception of organizations highlights a failure to consider the impact of monetizing consumer data by selling it to third party data brokers with a low level of security maturity.[24] It is also worth noting that 41% of organizations who believe it is easy for consumers to protect their data have themselves been involved in a data breach.

Investing in Data Privacy

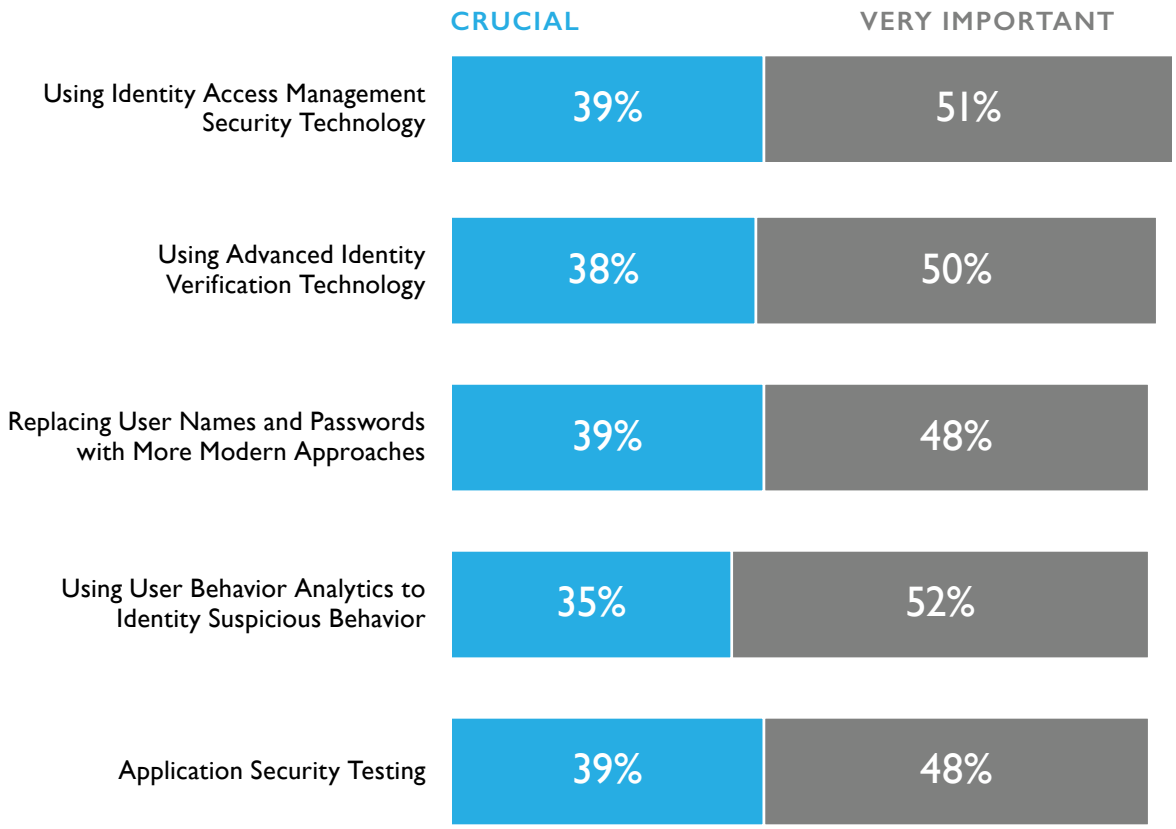
While organizations believe in the importance of tracking their data protection record—86% indicate they have quantitative measures in place—the gap between organizational perception of consumer trust and actual consumer trust is still significant. The gap may be a result of a workplace culture that deemphasizes the importance of security, particularly among business executives who may not understand the need to invest in data protection technologies, procedures, and training despite the fact that a breach has been proven to have a negative impact on the bottom line. Twenty-seven percent of business executives view security initiatives as having a negative return on investment (ROI). By comparison, only 7% of cyber security staff shares this view. Astonishingly, three quarters (76%) of business executives who view security initiatives as having a negative ROI have previously been involved in a publicly disclosed data breach. This suggests that despite the self-reported negative business impact that a breach carries, over one quarter of executives are tone deaf to modern security challenges and data breach implications, and have not learned from previous mistakes.

Twenty-seven percent of business executives view security initiatives as having a negative return on investment.

Although there are a substantial number of executives who view security initiatives as a poor investment, on the whole, organizations believe in the importance of investing in various technologies and security tools.

24 https://www.wired.com/story/exactis-database-leak-340-million-records/

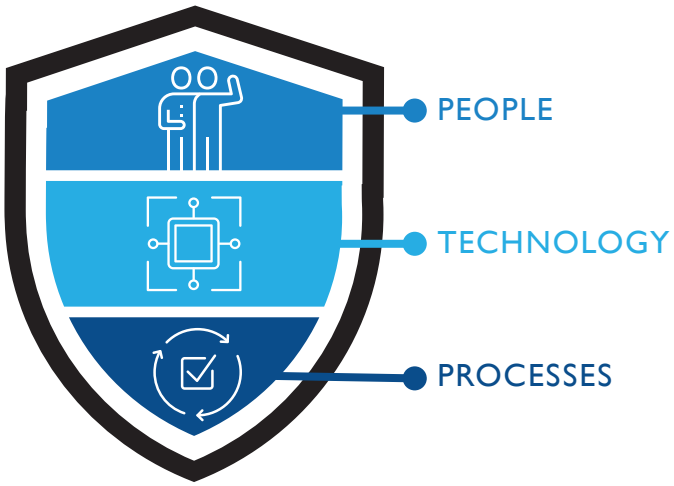
Exhibit 12: Importance of Implementation of Particular Technologies for Detecting and Blocking Threats to Consumer Data



Source: Frost & Sullivan, (N = 660)

Taken as an average, 88% of organizations believe it is very important or crucial to invest in the technologies listed above. This is a good sign because protecting PII in an organization requires a tripartite system of security that encompasses people, technology, and processes.

Exhibit 13: A Tripartite System of Security is Needed to Protect PII



Source: Frost & Sullivan

Technology is arguably the most important component of the tripartite system of organizational security and plays a key role in helping to secure PII. Organizations seeking to move into a demonstrable position of differentiating from competitors by providing better privacy protection must also look beyond the technologies in Exhibit 12 and implement additional next generation security technology tools. Technologies of importance include tools and controls that improve data sharing consent and privacy management, access controls capable of easily assigning and revoking access to privacy protected data in the organization, and lastly tools that incorporate automation to facilitate auditing and alert notification reporting to help organizations maintain compliance. As new technology is implemented to resolve security deficiencies, it is critical to implement regularly scheduled reviews to fine tune the technology pillar of organizational security operations.

Unfortunately only 60% of information security staff believes that non-security staff is trained to protect customer data.

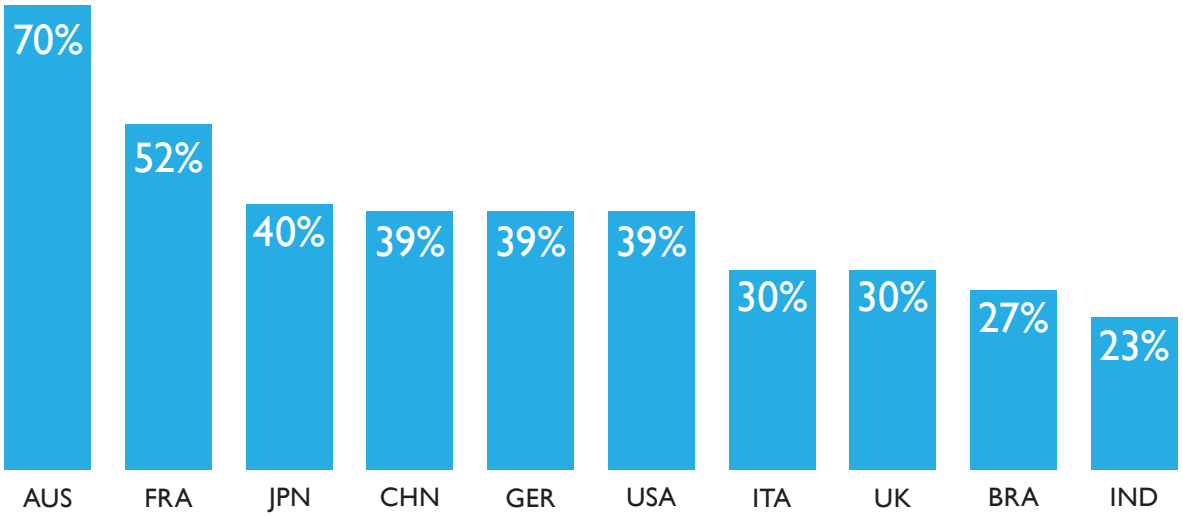
Since technology is the key pillar of the tripartite system of security, it also tends to be an area that organizations rely on most heavily to secure PII. However, some organizations rely almost exclusively on technology which leads to the question: are organizations investing in non-technical aspects of security that are also critical to protecting customer data? This is an important issue because a large number of data breaches occur as a result of social engineering targeted at non-security employees, which is better addressed with a combination of technology and security training. Unfortunately only 60% of information security staff believes that non-security staff are trained to protect customer data. Lack of security awareness training can weaken established processes for data protection or lead to new processes that fail to properly consider security implications.

Exhibit 14: Security Awareness Weak Spots

Source: Frost & Sullivan

According to information security professionals around the world, non-technical employees are the least prepared to protect consumer data. In Australia, information security professionals believe that 70% of non-technical employees are ill-prepared to protect consumer data and in France it's believed that over half of employees lack the necessary security training to protect consumer data.

Exhibit 15: Percentage of Non-security Employees that Information Security Professionals Claim ARE NOT Trained to Protect Consumer Data



Source: Frost & Sullivan, N = 336

The perceptions of information security professionals, those who are best able to objectively measure the security preparedness of non-technical colleagues, contrasts sharply with perceptions of business executives, **81% of whom believe that their non-security staff are trained to protect consumer data.**

THE FINAL WORD

It has been established that higher digital trust translates into higher revenue, which is why organizations intending to grow must enhance their digital trust credentials. Transitioning consumers into the high digital trust category will not happen quickly however, because there are many areas where organizations fail to understand the consumer experience.

While it might be said that there is an almost wilful ignorance among consumers about the exchange of data for free or freemium online services, it might also be said that organizations monetizing the data of paying customers wilfully hide those facts in 7,000-plus word T&C policies. Transitioning people from low and moderate digital trust into high digital trust consumers requires organizations to be concise and candid about how they protect data, if it is sold or shared, and how or if consumers who pay for products and services online can permanently opt out from data sharing.

Clearly communicating what organizational data protection policies are is a key factor of digital trust, a fact that is highlighted by 73% of consumers who stated they value easily accessible and understandable data protection policies. However, only 51% of consumers claim that organizations provide easily accessible and understandable information about data protection policies. The 22 point perception gap is indicative of a larger trend where organizations do not fully understand consumers.

Moving consumers along the digital trust continuum from low to high levels of trust is not a simple process; however several steps can be taken to reverse the trend of decreasing trust:

CULTIVATE A CULTURE OF SECURITY

Implement data protection policies that are in accordance with the world's strictest data privacy regulations. Ensure company-wide familiarity with security policies, including among non-technical staff to reduce the risk of data breaches.

START AT THE TOP

Too many business executives see security initiatives as a negative return on investment. Alert the C-Suite to the tangible business impacts of a breach and a loss of consumer trust.

COVER YOUR BASES

Consumers consider both social and technical factors when determining whether to trust an organization; be sure that your organization has the technical foundation in place to mitigate attacks and have a response team ready to minimize damage to consumer trust in the event of a breach.

KEEP IT SIMPLE

Clear communication from organizations around policies and data handling practices is critical for building trust. Far too many organizations overestimate the degree to which consumers can easily manage their personal data online. Present your policies in simple language, and provide important details without overwhelming the consumer.

Embracing these steps will begin the process of incremental increase in consumer trust among organizations at a time when this valuable commodity is dwindling. The degree to which these steps will disrupt the established corporate culture will vary between organizations, but all organizations stand to benefit from a future customer base that trusts companies with their personal information.

ABOUT CA TECHNOLOGIES

CA Technologies creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning, to development, to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at www.ca.com.

Co-authors of this paper include:

Jason Reed
Senior Industry Analyst, Cybersecurity,
Frost & Sullivan

Jarad Carleton
Principal Analyst, Cybersecurity
Frost & Sullivan

Frost & Sullivan would like to thank industry expert **David Duncan**, Vice President, Product & Solutions Marketing, Security Business Unit at CA Technologies for his contribution to this paper.

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost
myfrost@frost.com
www.frost.com