cpl.thalesgroup.com

THALES
Building a future we can all trust

2022 Consumer Digital Trust Index

Exploring Consumer Trust in a Digital World

In partnership with
WARWICK
THE UNIVERSITY OF WARWICK

#2022TrustIndex

Exploring Consumer Trust in a Digital World

By Prof. Carsten Maple, University of Warwick

The proliferation of digital has seen us move from bricks and mortar stores and banks to online services. And whilst digital has often improved experiences through its ability to make processes easier, faster and simpler, this shift has taken us on a rapid trust journey. In fact, for these digital services to be trusted, consumers must first be assured that they and their data is secure. And although trust used to take years to build, the new digital era has accelerated this process. However, it is important to remember that it only takes a second for trust to vanish.

Unfortunately, cybercrime seems to be more lucrative than ever, and the number and value of incidents reported maintain an upwards trajectory. In the UK, the National Fraud Investigations Bureau received more than 31,00 reports of cybercrime from individuals in 2020/2021, an increase of 15% over the same period the year before, while the reported cost of the crimes had risen nearly 80%. Most alarmingly, between 1 January and 31 July 2021, combining reports from individuals and organizations, 289,437 cases were reported, more than seven times the 39,160 cases reported over same period a year earlier - 31,000.

> **While the general public may not read the reports containing these cyber crime statistics, they will have read the mainstream media reports on attacks.**

Statistics from the National Fraud Database show that the number of cases of Identity Fraud in 2021 increased to more than 226,000, a jump of more than 22% over the previous year. To help combat this problem, the UK Government has established a National Cyber Force, comprising elements from the Ministry of Defence, GCHQ, the Defence Science and Technology Laboratory (Dstl) and the security services.

However, this problem is not restricted to the UK. According to the FBI, their Internet Crime Complaint Center received a record number of cases, 847,376, from the American public - a 7% increase from 2020. The estimated losses of these incidents exceed $6.9 billion, a jump of more than 60% on the previous year. In its latest report, the German Federal Office for Information Security (BSI), reported "a significant expansion of cybercriminal extortion method…The quality of the attacks also continued to increase significantly." At the end of May this year, France's data protection supervisor, Commission Nationale de L'informatique et Des Libertés (CNIL), released its annual report stating that they had received 5,037 notifications of personal data breaches, a 79% increase on the figures released a year before.

Cybercrime is also a major challenge in Japan, with reports of a sharp rise in reports of ransomware, the average demand of which is nearly 26 times higher than in the UK, according to a recent survey. In response to record cases of cybercrime, earlier this year Japan established a special investigation team in the National Police Agency to deal with serious cybercrime cases. This team comprises more than 200 experts to combat the issue. In Hong Kong, the Financial Services Development Council stated in late 2021 that the "financial services sector is heavily targeted by hackers and other cyber criminals", They report that Hong Kong saw an almost six-fold increase in cybercrime, with reported incidents rising from 2,206 in 2011 to 12,916 in 2020, with the annual cost increasing 20 times, from HK$148 million in 2011 to HK$2.96 billion in 2020. Earlier this year, Singapore's Minister for Communications and Information, Josephine Teo, discussed the governments concern regarding cybercrime, as cyber threats to Singapore have become more prevalent, with a 73 per cent increase in data breach and ransomware incidents in 2021 compared to the previous year.

In Japan, residents will have been concerned that Japanese telecommunications company Nippon Telegraph & Telephone (NTT), the fourth largest telco in the world 55th in the Fortune Global 500, suffered a data breach in March of this year. The size of the organization being breached will have

Professor Carsten Maple

University of Warwick

Professor Carsten Maple is Professor of Cyber Systems Engineering and Director for Cyber Security Research, University of Warwick. He is also the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research at the University and Professor of Cyber Systems Engineering in WMG. He is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. Carsten has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. Carsten is also co-author of Cyberstalking in the UK, a report supported by the Crown Prosecution Service and Network for Surviving Stalking. His research has attracted millions of pounds in funding and has been widely reported through the media. He has given evidence to government committees on issues of anonymity and child safety online. Additionally he has advised executive and non-executive directors of public sector organizations and multibillion pound private organizations.

been a concern, though records of less than a thousand customers were leaked. The size of breach is orders of magnitude smaller than the breach of the systems of the Line app in the same month, which saw the compromise of personal information linked to nearly 86 million users in Japan. In June last year, several large government agencies in Japan, including the ministries of Land, Infrastructure, Transport and Tourism, as well as Narita International Airport, were reported to have suffered data breaches. In Singapore, many of its 5.6 million residents will be aware of recent attacks on health databases. Last year attackers compromised the personal medical records, including details of serious illness and treatment plans, of up to 73,000 patients of the Eye & Retina Surgeons clinic. This followed a leak of information the previous year in which patient data, including medication prescribed, of 1.5 million people in Singapore, including the country's Prime Minister Lee Hsien Loong, were breached in the attack on the systems of health provider SingHealth

While the general public may not read the reports containing these cyber crime statistics, they will have read the mainstream media reports on attacks. Within the last year, in the UK alone, they will have read how the Foreign, Commonwealth and Development Office was breached, and that the Labour Party members data was breached.

> **There are significant potential problems if customers become desensitised to security breaches.**

In the US, people will have heard of the attack on Indiana COVID tracing survey in which the personal information - including names, addresses, birth dates, email, gender, ethnicity and race – of 750,000 people was accessed. In Brazil last year, citizens would have heard the news that the breach of a major Brazilian database appears to have exposed the CPF number (the tax identity registered with the Brazilian Revenue) and other confidential information of millions of people. The data that was released was reported to have contained detailed information on more than 100 million vehicles, 40 million companies, and 220 million people. In an attack with global impact, around 20% of all Facebook users (533 million people) had their account details shared on a cybercrime forum in 2021.

The data contained information users had entered in their profiles including Facebook ID numbers, profile names, email addresses, location information, gender details, job and educational data. Beyond these company and government attacks, the public will have heard of numerous reports of vulnerabilities from Heartbleed to SolarWinds.

As well as reading about attacks, the public have also experienced the impact of attacks. It isn't many years ago that the Wannacry attack had a major impact on the UK's NHS, forcing many patient appointments to be lost. More recently the Tesco attack that impacted its website and app leaving thousands of customers unable to access their online shopping service. In the US, people will have experienced fuel shortages caused by the Colonial Pipeline and the Kayesa hack that shut down payment terminals.

Against this global backdrop of cybercrime, its unsurprising that academics are asking whether consumers are becoming desensitised to security breach notifications. Others are questioning how much trust citizens have in organizations and governments to protect their information online.

There are significant potential problems if customers become desensitised to security breaches or fail to trust organizations to adequately protect their information, and this would have ramifications for industry, government and regulators. If citizens feel that breaches of information are part and parcel of interacting online, then there is a possibility that they will be less concerned about their own security practices as well as those of online organizations.

> **Consumers are less likely to relax cyber security practices if they feel that they are adding value to the effort in protecting their information.**

Clearly this would be a perilous stance to take, but often acting securely is seen as requiring effort – remembering different passwords for different accounts, regularly changing passwords and so forth. If there was an inclination that these cyber hygiene practices have little overall impact because it is believed to be irrelevant how strong the password is if it is compromised at the organizations end, then the effort may not be deemed worth the protection.

Of course, the benefit of good consumer security practices is well-understood by industry, government and regulators but if the consumers don't experience the value, behaviours and attitudes could change. This would have consequences for security professionals in industry since they will find it harder to convince boards to invest in cyber security. Governments would feel the consequences as losses are aggregated across citizen populations, and regulators would lose a key argument in the need for strong regulations and enforcement powers.

Consumers are less likely to relax cyber security practices if they feel that they are adding value to the effort in protecting their information. To feel that they are adding value, they must be confident that the organizations that they interact with online are doing their best to protect consumer information. As such, this survey is both timely and important. In the first survey of its kind, Thales aim to understand citizen behaviours, preferences and trust in online environments and produce a Trust Index.

The survey is not only unique in the issues it strives to explore, but also on the scale and coverage of the survey. More than 21,000 citizens were surveyed across 11 countries and 5 continents to provide novel insights into consumer opinions and behaviours. The survey examines whether, and identifies how, citizens react after their information is exposed when a company is compromised. This provides insight into whether they are becoming desensitised. The survey also explores, across a range of sectors, the extent to which citizens trust organizations, and the security controls they feel should be employed. The insights that are obtained will surprise many – it certainly made me reconsider what I thought I knew.

Key findings

Digital trust varies across the world

The most trusting nations:

95% Brazil
92% Mexico
91% UAE

The least trusting nations:

23% Germany
20% Australia
20% UK
20% France

Digital trust varies across industries

The most trusted industries:

42% Financial Sector
37% Healthcare
32% Consumer Technology

The least trusted industries:

18% Social Media
14% Governments
12% Media and Entertainment

11%

of companies took up to 6 months or a year (5%) to inform the consumer about a data breach

21%

of consumers stopped using the company who suffered a data breach, of whom 42% requested they delete their information

54%

of consumers believe that companies should be forced into mandatory data protection controls like encryption and two-factor authentication following a data breach

33%

of consumers globally have already become victims of a data breach

82%

of data breach victims saw a negative impact on their lives

Contents

Part 1: A New Era of Trust

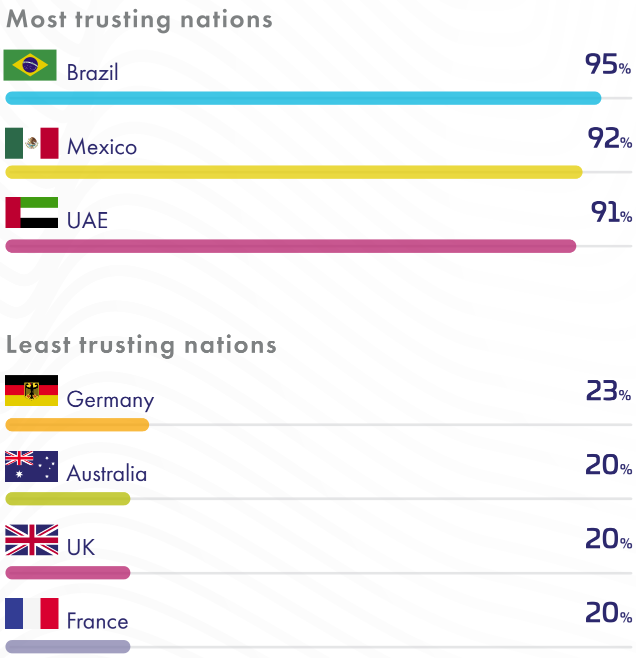
Data breaches plague organizations across the world, with a third (29%) of organizations suffering a data breach over the last 12 months. But this isn't a new phenomenon, we have seen these numbers year after year, despite repeated warnings of the risks associated with the loss of data. So, is it a case that now there is a growing acceptance amongst organizations that the risk no longer outpaces the reward, and do consumers trust that they will do the right thing when it comes to securing data?

Today, organizations understand that it is no longer a case of if but when a data breach will occur, and this appears to be translating to consumers. Despite being more aware than ever about how their data, whether personal identifiable information or not, is being used and the risks associated with it being stolen, coupled with constant news of data breached occurring, four in five (82%) consumers continue to trust online digital service providers to protect their personal data at least somewhat; 15% completely trusting of them.

This level of trust does vary across the world, with consumers in Brazil (95%), Mexico (92%) and the UAE (91%) reporting the highest levels of trust in online services. By contrast, Germany has the lowest reported level of trust, with 23% of consumers not trusting, while in Australia, France and the UK, 20% of consumers don't trust online services with their data.

When it comes to age, digital natives (18-34) are more trusting to online digital services companies than those over 55; 87% vs 74%. In fact, while only one in 10 (11%) of digital natives claimed not to trust online digital services to secure their personal data, double (22%) of those aged over 55.

Percent of consumers who trust the digital services providers with their personal data.



82%

consumers continue to trust online digital service providers to protect their personal data at least somewhat;

87%

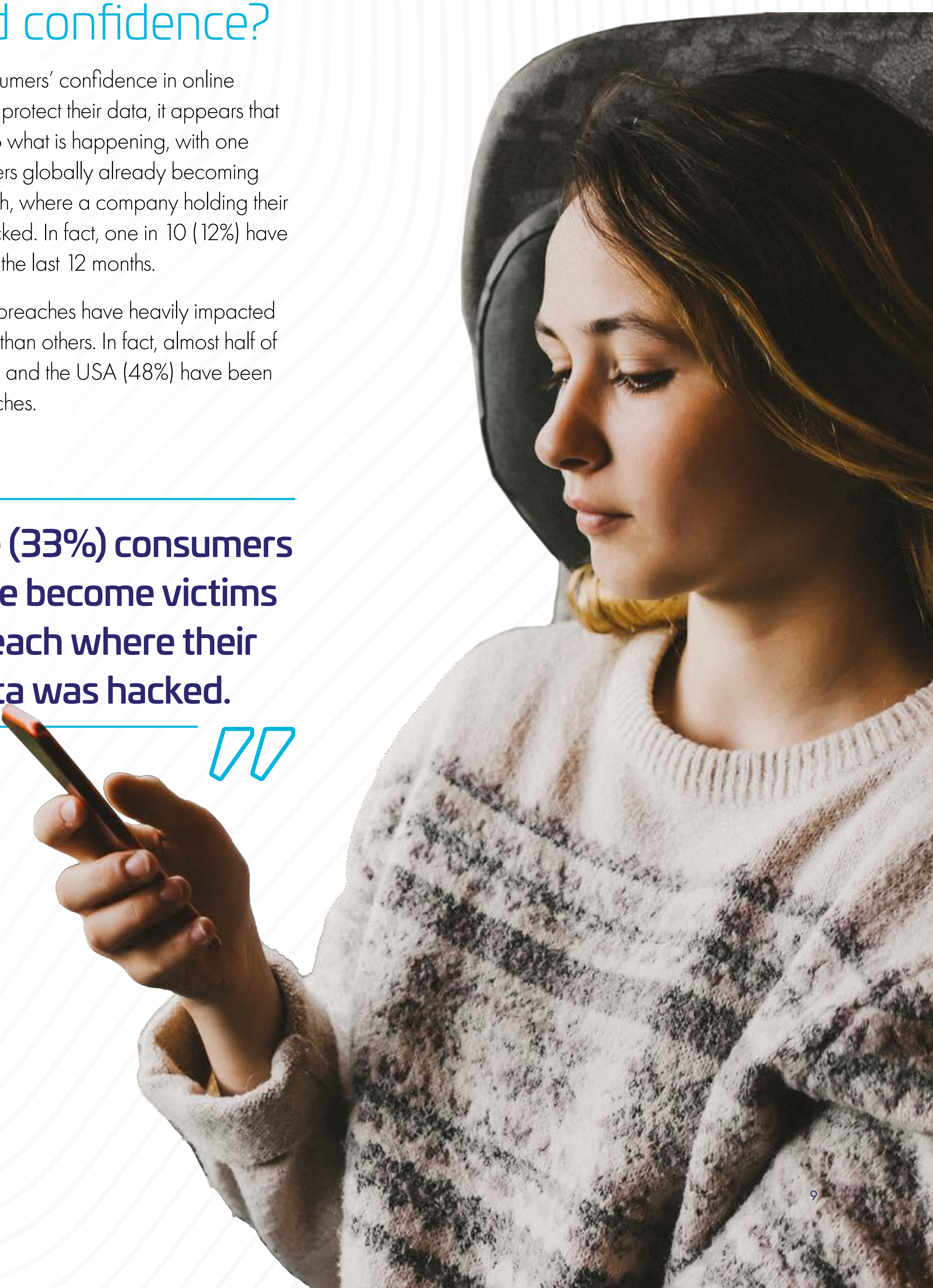
of 18-34 year olds up are more trusting to online digital services companies than those over 55

Misplaced confidence?

When it comes to consumers' confidence in online organizations ability to protect their data, it appears that it may be misaligned to what is happening, with one in three (33%) consumers globally already becoming victims of a data breach, where a company holding their personal data was hacked. In fact, one in 10 (12%) have experienced this within the last 12 months.

Geographically, data breaches have heavily impacted some consumers more than others. In fact, almost half of those in the UAE (49%) and the USA (48%) have been affected by data breaches.

> **One in three (33%) consumers globally have become victims of a data breach where their personal data was hacked.**



> Businesses have no choice but to improve their security if they want to address frustrated consumers that don’t believe the onus is on them.

Trust in industries

The degree of trust that consumers have when it comes to the security of their personal information varies by industry. Industries where consumers have the greatest level of trust Banking & Financial (42%), Healthcare Providers (37%) and Consumer Technology Companies (32%) to the list for being trustworthy to secure their personal information.

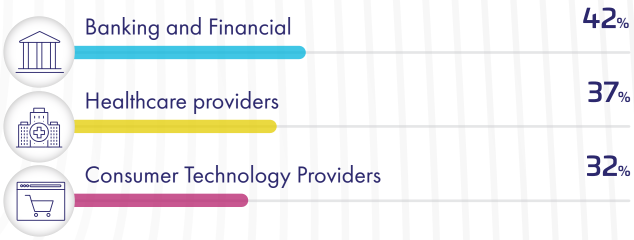
On the opposite side of the scale, were Social Media companies (18%), Government (14%) and Media & Entertainment organizations (12%) all had the lowest level of consumer trust. Despite being included as one of the most trustworthy industries, a significant proportion of respondents (14%) had low trust in government. This could be an indication of what has happened on the political landscape across, Brazil (25%), USA (24%), Mexico (21%) and the UK (19%) showing their lack of trust when it comes to their government to protect their personal information.

While it often takes many years to build trust, it can be lost very quickly. Despite it being several years since the Cambridge Analytica scandal, the fallout of from the misuse of users' personal data continues to roll-on.

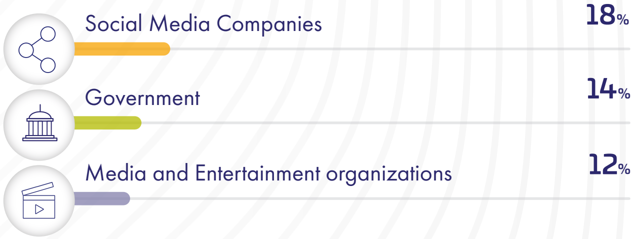
The harvesting of Facebook data of 87 million people being used for advertising during election, has tarnished the industry, with nearly one in five (18%) of consumers globally giving them a low trust score.

Notably, this lack of trust rises to over a quarter (29%) in the UK, and a quarter in Australia (25%) and the USA (24%), indicating that it may take years for trust to be rebuilt.

Top three trustworthy industries



Top three least trustworthy industries

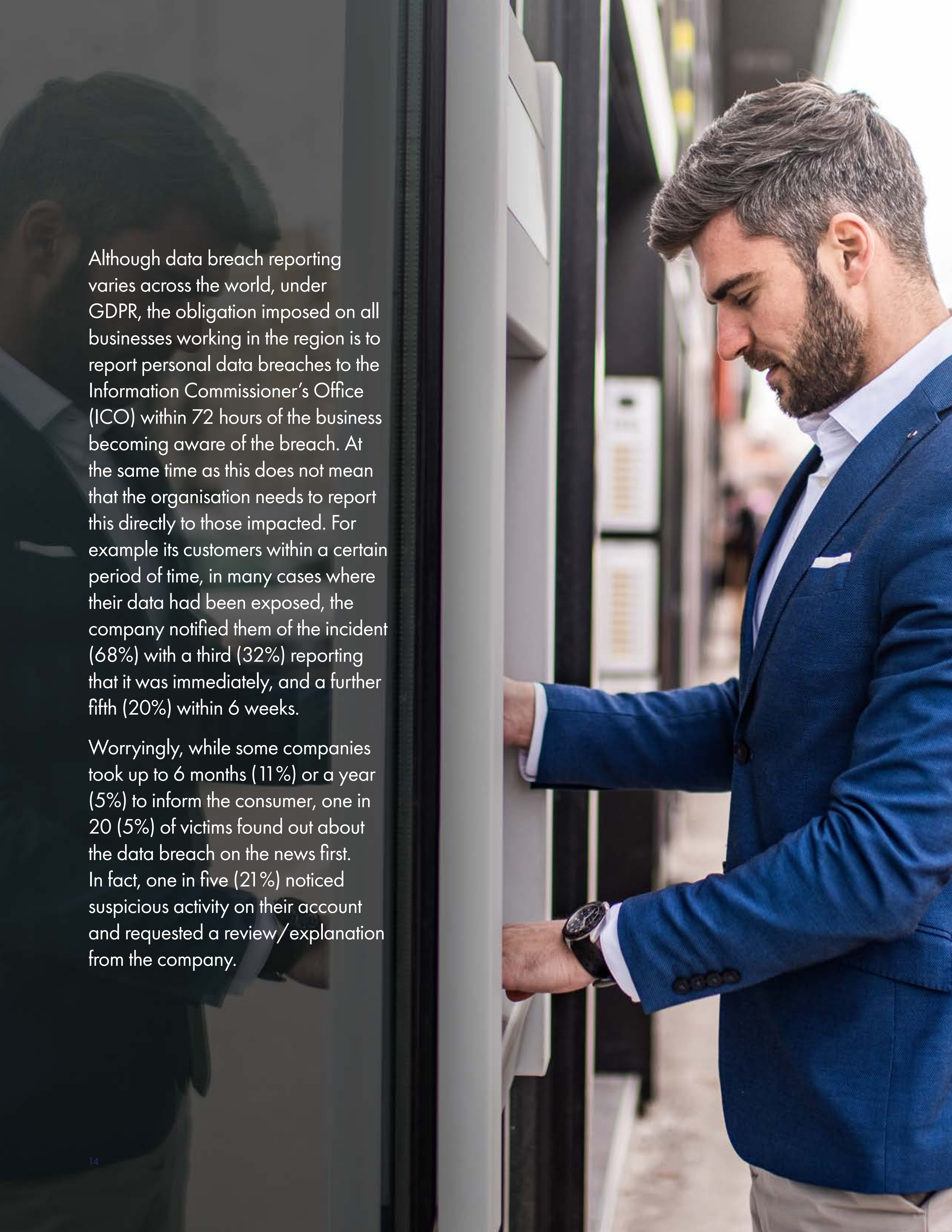


Distrust in Social Media Organizations

This comes as data breaches affecting online services have made consumers increasingly concerned about personal data held by digital service providers, particularly social media (62%), banking (60%), and email (56%) providers. Consumers in Brazil (76, 82%, and 70% respectively) and Singapore (74%, 81%, and 72% respectively), are particularly concerned about data security for these online digital services.

> **Data breaches affecting online services have made consumers increasingly concerned about personal data held by digital service providers.**

Part 2: The impact



Although data breach reporting varies across the world, under GDPR, the obligation imposed on all businesses working in the region is to report personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of the business becoming aware of the breach. At the same time as this does not mean that the organisation needs to report this directly to those impacted. For example its customers within a certain period of time, in many cases where their data had been exposed, the company notified them of the incident (68%) with a third (32%) reporting that it was immediately, and a further fifth (20%) within 6 weeks.

Worryingly, while some companies took up to 6 months (11%) or a year (5%) to inform the consumer, one in 20 (5%) of victims found out about the data breach on the news first. In fact, one in five (21%) noticed suspicious activity on their account and requested a review/explanation from the company.

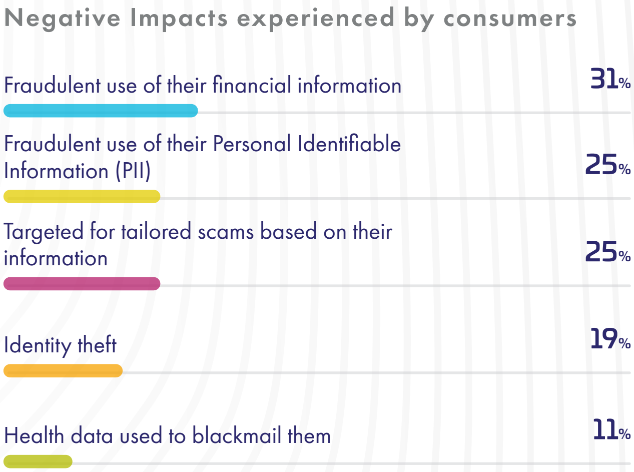
A big impact on consumers

While a fifth (18%) of those that had their data exposed because of a data breach did not experience any negative impact, the vast majority (82%) reported being affected in one or more of the following ways:

When it comes to consumers by nation, the impact of a data breach is not shared equally. In fact, 94% of those in UAE, 90% in Mexico and 87% in Brazil reported that a data breach had negatively impacted them - significantly higher than consumers in the UK (65%), Japan (69%) and USA (75%).

Despite many data breach victims having seen some negative impact following the incident, four in five (79%) have continued to use the company that suffered the breach rising to nine in ten in Hong Kong (91%), Singapore (89%), and the UAE (88%).

However, 21% stopped using the company, of whom 42% requested they delete their information, 16% reported them to a financial regulator, 9% are considering taking legal action, and 8% have already taken legal action against the company. Over a third (36%) did not take any further action.



Negative Impacts experienced by consumers

> **Worryingly, while companies took up to 6 months (11%) or a year (5%) to inform the consumer.**

21%

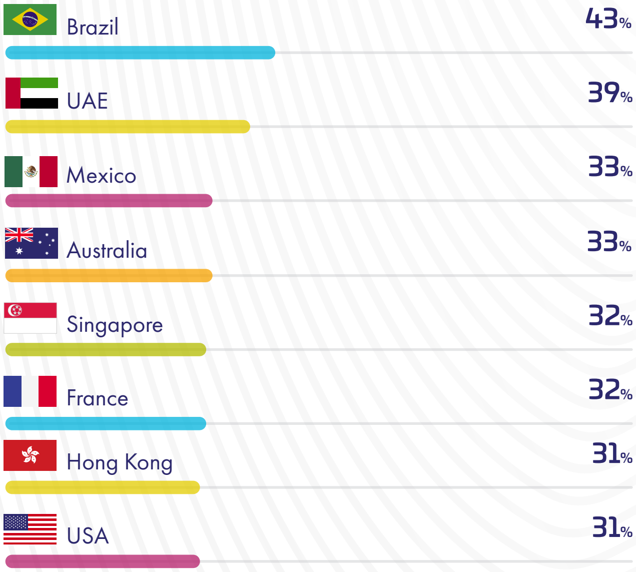
stopped using the company that suffered the breach

Criminal activity by country

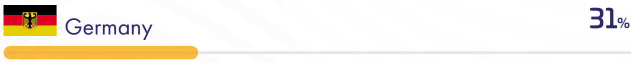
When it comes to the types of activities criminals were undertaking in each region, the largest impact was fraudulent use of their financial information. Interestingly, only Germany, Japan and the UK reported higher stats for other techniques.

> **The largest impact was fraudulent use of their financial information.**

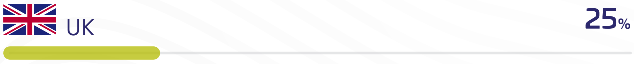
Fraudulent use of their financial information



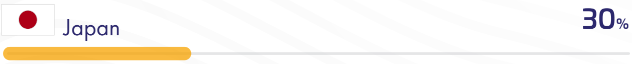
Fraudulent use of their Personal Identifiable Information (PII)



Targeted for tailored scams based on their information



Identity theft



Part 3: Action

Data breach victims are more likely (96%) to take additional precautions to protect their personal data, versus 88% among those that have not knowingly been victims of a data breach.

While organizations have a responsibility to implement robust security practices, it is equally important that consumers look to protect themselves against external threats too. In fact, one in three (33%) consumers worldwide see password protection as essential for accessing online services, while half (52%) always use this feature when available they will still use a site if it's not available. The same can be said for other security features such as two-factor authentication (63%), encryption (52%) and biometric authentication (54%).

Notably though, consumers expect different security features for different types of online services. Take banking for instance, consumers understandably want more enhanced security features for banking services to protect their sensitive data. Two-factor authentication is the most in-demand security feature for online banking, 68% of consumers think this should be offered, this is followed by password protection (53%), encryption and biometric authentication (both 47%). There are also differences by market, we can see a much higher demand for biometric authentication for banking services in some markets such as Brazil (67%), Mexico (61%), Singapore (59%) and the UAE (58%).

Similarly, since email is often the key to many other services, password protection is desired by 57%, and other features such as two-factor authentication (49%), encryption (35%), and biometric authentication (25%) are slightly less in-demand. A similar pattern can be observed with most other types of online services.

Spending extra time securing themselves

When it comes to protecting themselves, Banking & Financial Services are where the majority of consumers (69%) are likely to spend most of their time adding additional security measures to protect and secure their personal data they store with them as a result of organizations facing data breaches. This is followed by email (54%), social media (48%) and shopping (44%).

Despite having access to personal data, only a third (33%) of consumers spend time implementing additional security measures in healthcare, while only a quarter (24%) spend it travelling.

> **Whilst organizations have a responsibility to implement robust security practices, it is important that consumers look to protect themselves against external threats too.**

What should happen to organizations?

When it comes to what should happen to organizations that have suffered a data breach, while compensation to the victims comes a close second, consumers across the world are in agreement that better encryption and access management protocols should be implemented.

54%
Should implement mandatory data protection controls like encryption and two-factor authentication

43%
Should be responsible for finding victims data and paying to have it returned

53%
Should offer compensation to victims

42%
Should be subject to more stringent regulation e.g., be monitored for 12/24 months

46%
Should employ more specialists to ensure it doesn't happen again

31%
Should be been given large fines

Conclusion

Through this large-scale, global survey we have discovered new insights into citizen reactions to data exposures – both in personal behaviours and in attitudes towards companies that were the source of the compromise, and the levels of trust that they place in industry and government.

Governments recognise the importance of making cyber space safe and secure. In particular, they recognise the importance that citizens play, alongside industry, governments and regulators.

Since 2005, the Office of the Government Chief Information Officer in Hong Kong, Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination have worked together to conduct an annual "Build a Secure Cyberspace" promotion campaign. This aims to raise public awareness in information security through a series of activities, including a media campaign, a series of competitions, and holding thematic seminars and school visits. In 2016, the Singaporean Government launched its Cybersecurity Strategy with four Pillars including one to create a safer cyberspace. Their recent Masterplan, launched in 2020, outlined plans to support individuals to strengthen their cybersecurity posture.

The aim is to Empower a Cyber-Savvy Population, enabling Singaporeans to "live, work and transact in the digital domain securely, having taken steps to protect themselves online." In the UK, the National Cyber Security Centre (NCSC) was established in 2016 to help make "Britain the safest place in the world to be online". As part of its work, the NCSC provides internet security guidance to organizations and citizens. This includes the Cyber Aware programme that provides citizens with "advice on how to stay secure online" as well as advice such as password management and general cyber hygiene.

> **Social Media companies have the most significant issue with trust since 1 in 2 respondents reported having no trust at all in these companies keeping their information secure.**

The US launched its first National Strategy to Secure Cyberspace in 2003, under the George W. Bush administration. In this report the US Government declared that "all users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace." The strategy outlined plans to provide a "comprehensive national awareness program to empower all Americans - businesses, the general workforce, and the general population - to secure their own parts of cyberspace" and to develop "adequate training and education programs" to protect cyberspace.

What's more, major cyber incidents such as SolarWinds and Colonial Pipeline, were seen as the driving force behind President Biden signing an Executive Order in May 2021. Aimed at improving the nation's cyber security and protect federal government networks, the order ensures that government agencies now must practice good cyber hygiene; mandating that multi-factor authentication and encryption were introduced within 180 days. The order highlighted the importance of maintaining a good cyber hygiene posture is a shift in mitigating threats – instead of reacting to an incident, basic cyber hygiene can help you to proactively prevent ransomware attacks before they occur.

Each of these strategies, and their successors and supporting action plans, highlight the need for citizen-industry collaboration and trust. Indeed, as part of the UK Digital Strategy, released in 2017, the UK Government committed to "retain the trust of citizens in online public sector services and systems, ensuring that appropriate levels of security are implemented across the public sector." This survey has examined the level of trust citizens across the globe place in their respective governments.

The success of the UK Government in achieving this may be questioned since 11% of all UK respondents to this survey stated, on a scale of 0-10, that they had "no trust at all" in the security of the of digital services the Government offers and protection of their personal information. This compared unfavourably to all other sectors, except for social media companies for which 14% of UK respondents had no trust at all. Looking at international comparisons, only the USA and Brazil governments fare worse, with 14% and 13% respectively, of citizens having no trust at all in their governments. Further, this is significantly worse than Singapore and the UAE in which only 2% of respondents stated they had no trust at all, and worse than other European countries; France and Germany each had only 3% of respondents declare no trust at all in their government's cyber security capability in this regard.

Trust in other organizations is also much lower than many industries would want. Social Media companies have the most significant issue with trust since 1 in 2 respondents reported having no trust at all in these companies keeping their information secure. Conversely, only 2% of respondents felt the same way about healthcare providers, such as doctors and hospitals, with 1 in 13 trusting these organizations completely. The banking and finance sector also fared well with only 2.5% having no trust at all but 1 in 11 people having complete trust.

This report provides other key information that will be of interest to governments across the globe. Most startling for me was the revelation of how prevalent it was for health data to be used in blackmail cases. Of those impacted by a data breach, 11% reported that healthcare data had been used to blackmail them. This significant level of extortion sits against a huge global increase in the use of ransomware to extort money from individuals and organizations. It would appear that criminals are finding cyber extortion extremely lucrative.

> **Interestingly, the responses indicate that citizens are more concerned that action should be taken to support protection against future attacks than financial or data restitution.**

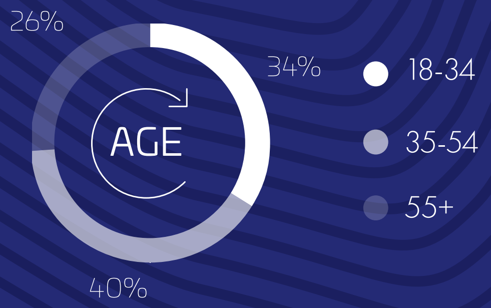
Regulators around the globe have been established and empowered to provide guidance to government and industry and penalise them in cases where regulations have been contravened. This survey provides an interesting insight into what citizens feel that should happen to organizations that have experienced a security breach. Interestingly, the responses indicate that citizens are more concerned that action should be taken to support protection against future attacks than enabling financial or data restitution. Globally 54% feel that organizations should have to implement mandatory data protection controls whereas only 53% feel compensation should be offered to victims; 46% feel organizations should employ more specialists to ensure it doesn't happen again. Of interest to regulators is that by far the lowest priority of action to take against firms that have suffered is to give them large fines, the most frequent action of regulators around the world – only 3 in 10 believed this should be done.

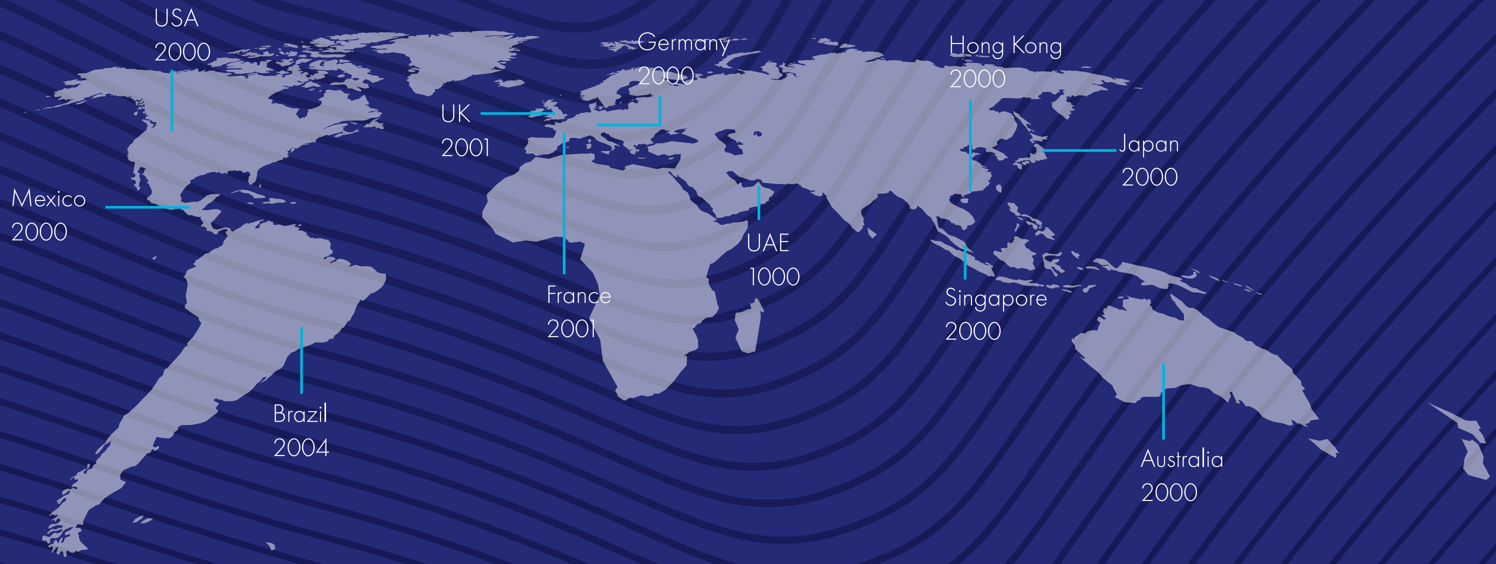
The issue of whether citizens were becoming desensitised to cyber breaches was raised in the foreword of this report. The survey has managed to shed some light on the actions of respondents in response to their own data being exposed. Incredibly 8 out of 10 people would still use the service, even after it had been compromised to expose their data. The figures vary across countries, but remains high across the globe. France and the UK are the nations whose citizens are most likely to cease using a service, with 71% and 73% continuing to use the service, whereas the highest inertia is seen in Singapore and Hong Kong with 89% and 91% continuing to use the service, respectively. Of those who did cease to use the services, the majority – 6 in every 10 people – took some kind of action. While requesting that their information was, as expected, the most common action it is surprising that more that 17% of people that had stopped using the service had already taken legal action or were considering doing so. The responses to these questions show a polarisation in behaviours following a breach. While the vast majority continued to use the service, a reasonable minority have taken, or are considering taking, very serious action. This revelation, like many others in this report is both useful and encourages further research.

> **Incredibly 8 out of 10 people would still use the service, even after it had been compromised to expose their data.**

Demographics

A total of 21,006 adult consumers were surveyed across 11 countries and 5 continents, 2000 in the UK, the USA, Germany, France, Mexico, Brazil, Japan, Singapore, Hong Kong, Australia and 1000 in the UAE





Moving Ahead

The line between our online and offline lives is blurring. In a highly interconnected world, societal well-being, economic prosperity, and national security are impacted by the internet. With this report Thales is aiming to empower individuals and organizations to own their role in protecting their cyberspace. If everyone does their part – implementing stronger security practices, raising community awareness, educating people, following good cyber hygiene – our interconnected world will be a safer and more resilient place for everyone. This is the only way to keep people safe from attacks on their data, personal information, finances and infrastructure.

It is clear that cyberattacks are on the rise and adversaries are developing more sophisticated cyberattacks. Maintaining a good cyber hygiene posture is a shift in mitigating threats – instead of reacting to an incident, basic cyber hygiene can help you to proactively prevent attacks before they occur. Even if an attack should occur, good cyber hygiene practices can help organizations control and reduce the impact. As the organization becomes more mature, it can implement more advanced cybersecurity controls to block bad actors from hijacking their sensitive, valuable data.

There are three key pillars for a truly holistic approach to data security to be implemented across an entire organization:

Discover

Discover where data resides on premises or in the cloud and classify its sensitivity and importance based on internal policies and external regulations.

Protect

Protect sensitive data at rest, in motion and in use with advanced encryption and tokenization, making the data useless if it is lost or accessed by unauthorized individuals.

Control

Control access to sensitive data with authentication and centralized key management across on-premises and hybrid cloud environments. This simplifies data-centric security, ensures regulatory compliance, and reduces risk across an organization.

ONLINE GROCERY
5+
Offer
Orange Pack
Any 2 for 2.50
Write a review >
More information >
$1.85
Add
Orange Minimum 5 Pack
Write a review >
More information >
$1.50
Add
5+
Oranges Each
$0.30
Sweet Easy Peeler Pack 600G
Write a review >
More information >
$1.35
Add
Raspberries 150G
Write a review >
More information >
$2.00
Add
Sweet Apple Mineral 5 Pack
Write a review >
More information >
$0.95
Add

THALES

Building a future we can all trust

Contact us

For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/data-trust-index