Consumers vs Businesses

Consumers are increasingly aware of online security risks, but hold businesses responsible for data breaches
Consumers are increasingly aware of online security risks, but hold businesses responsible for data breaches.

Consumers are putting the responsibility for protecting their personal data firmly at the hands of the organizations holding their data – and not themselves, this is according to Gemalto’s 2016 Data Breaches and Customer Loyalty report.

According to the 9000 consumers surveyed in Australia, Benelux, France, Germany, Russia, UAE, Saudi Arabia, India, Japan, United Kingdom, and United States, 70% of the responsibility for protecting and securing customer data, lies with companies and only 30% of the responsibility with themselves. Yet, less than a third (29%) consumers believe companies are taking protection of their personal data very seriously. This comes as consumers are becoming increasingly fearful of their data being stolen, with 58% believing it will happen to them in the future. More than 4.8 billion data records have been exposed since 2013 with identity theft being the leading type of data breach accounting for 64% of all data breaches.

80% use social media, despite 59% believing these networks pose a great risk. 87% use online or mobile banking, with 34% believing they leave them vulnerable to cybercriminals.

Adult sites (39%) and torrent sites (37%) are also believed to house considerable risks.
Key Findings

Where Consumers See Most Risk

Despite becoming more aware of the threats posed to them online, only one in ten (11%) believe there are no apps or websites out there that pose a great risk to them and consumers are not changing behaviour as a result.

Consumers are also more likely to shop online during busy commercial periods such as Black Friday and Christmas (2% increase online versus -2% decrease in store), despite 21% admitting the threat of cybercrime increases a lot during these periods.

Consumers Attitudes on Data Breaches

Nearly six in ten consumers believe they will be a victim of a breach at some point, and organizations need to be prepared for the loss of business such incidents may cause. The majority of consumers say they would stop using a retailer (60%), bank (58%) or social media site (56%) if it suffered a breach, while 66% say they would be unlikely to do business with an organization that experienced a breach where their financial and sensitive information was stolen.

How Data Breaches Affect Consumers

The study found that fraudulent use of financial information has affected 21% of consumers, with others experiencing fraudulent use of their personal details (15%) and identity theft (14%). More than a third (36%) of those who have been a victim of a breach put this down to a fraudulent website. Clicking a bad link (34%) and phishing (33%) were the next highest methods consumers were caught out by. In keeping with the theme of putting the blame at the organization’s hands, over a quarter (27%) attributed the breach to a failure of the company’s data security solutions.

Lack of security measures influence consumer confidence

The lack of consumer confidence could be due to the lack of strong security measures being implemented by businesses. Within online banking, passwords are still the most common authentication methods – used by 84% for online and 82% for mobile banking, and more advanced transaction security the next highest for both (50% and 48% respectively). Solutions like two-factor authentication (43% online and 42% mobile) and data encryption (31% online and 27% mobile) trail behind.

Similar results can be seen in both the retail space, with only 25% of respondents that use online retail accounts claiming two-factor authentication is used on all their apps and websites, and in social media, with only 21% using the authentication for all platforms. Only 16% of all respondents admitted to having a complete understanding of what data encryption is and does.
Consumers’ online accounts
The majority of respondents actively use online accounts. 87% have online/mobile banking, 80% have social media accounts and 79% have online retail accounts.

This suggests that most consumers are doing a range of activities online and it is likely that a number of companies are going to hold consumers’ personal data.

Fig 1: Which of the following do you actively use?
The greatest risks to data protection and security

The majority (89%) of respondents believe that certain apps/websites are leaving their personal information exposed.

Around six in ten (59%) respondents feel that social media apps/websites expose them to the greatest risk, although most do actively use online social media accounts.

More than one in three (34%) also feel that banking apps/websites leave them vulnerable, but the majority actively use them.

Most consumers are aware of the risks that online accounts pose to their personal information, but are continuing to actively use them regardless.

Fig 2: Which apps/websites do you feel expose you to the greatest risk in the protection and security of your personal information?
Use of passwords for online accounts

Over half (53%) of surveyed consumers use the same password across some or all of their accounts.

More than one in ten (13%) admit to using the same password across all of their online accounts.

In general, consumers are conscious of the risk that using online accounts can pose to their personal data (figure 2), but are leaving themselves more vulnerable by using the same passwords across multiple accounts.

Fig 3: Do you tend to use the same password across all of your accounts?
Victims of a breach

Repercussions of an online breach

Many respondents would stop using social media sites, retailers or banks if they were to suffer an online breach.

Six in ten (60%) would stop shopping with a retailer and a similar proportion would stop using a bank (58%) or a social media site (56%).

For around three-fifths (58%) of surveyed consumers, they are worried that at some point their online personal information will be stolen.

For most consumers, they believe that they will be a victim of a security breach and they intend to punish the organisation they trusted to store their personal data, if it were to happen.

Fig 4: Analysis of respondents who agree with the above statements
Victims of a data breach

Around one fifth (21%) of respondents have been the victim of fraudulent use of their financial information and slightly fewer have experienced fraudulent use of their PII (15%) and/or identity theft (14%).

According to those that have been a victim of a data breach, visiting a fraudulent website (36%), clicking on a fraudulent web link (34%) and failure of an organisation’s security solutions (27%) are amongst the causes for the breach.

Many consumers are victims of breaches and there are a range of ways they can experience one, including others’ negligence.

---

Fig 5: Have you been a victim of the following?

- Identity theft: 14%
- Fraudulent use of your financial information: 21%
- Fraudulent use of your Personal Indentifiable Information (PII): 15%

Fig 6: Which of the following are the most likely causes for you being a victim of a breach?

- Visiting a fraudulent website: 36%
- Clicking a fraudulent web link: 34%
- Phishing: 33%
- Failure of an organisation’s security solutions: 27%
- Downloading an attachment from an email: 27%
- Receiving a scam phone call: 23%
- Downloading an application: 21%
- Stolen wallet: 21%
- Skimming: 20%
- I don’t know: 12%
Taking legal action after a breach

Almost half (48%) of those surveyed have either taken legal action against the parties involved in exposing/taking their personal information, or are considering it (figure 7). Only 7% of respondents would not consider legal action in the future if they were a victim of a breach.

A large proportion of consumers would and do take legal action against those responsible for a data breach, whether that be the fraudsters or the organisation they entrusted.

**Fig 7:** Have you taken legal action against any of the parties involved in exposing/taking your personal information?

- Yes, I have done so against the fraudsters: 52%
- Yes, I have done so against the company that was breached: 15%
- Yes, I have done so against both the fraudsters and the company that was breached: 18%
- No, but I am considering doing so: 9%
- No, and I am not considering doing so: 6%

**Fig 8:** If in the future you were a victim of a breach, would you take/consider taking legal action against any of the parties involved in exposing your personal information?

- I would take legal action against the fraudsters: 34%
- I would take legal action against company that was breached: 22%
- I would take legal action against both the fraudsters and the company that was breached: 8%
- I would consider taking legal action: 7%
- I would not take legal action and would not consider doing so: 29%
Why consumers take legal action after a breach

The most likely reason why consumers that experienced a data breach took legal action, was that they felt they should out of principle (41%).

Other reasons include: it was such negligence that they felt they had to take action (35%); family and friends have previously so they knew they could too (21%); and there was media hype which spurred them to go down the legal route (17%).

As more people take legal action against the parties involved in exposing/taking their personal information, more consumers are likely to feel empowered to follow suit – joining those that use the law because they feel it is the right thing to do.

Fig 9: What prompted you to take legal action against any of the parties involved in exposing/taking your personal information?
Likelihood of being a victim of a breach

Over a third (35%) of respondents believe that they will become the victim of a breach at some point. 26-31% are unsure if they will be a victim or not.

During a high profile commercial event, approaching a quarter (22%) of those surveyed think that they are likely to suffer from a data breach.

This suggests that while most do not believe they will become a victim in the future, a significant proportion think that it will happen to them.

Fig 10: How likely do you feel you are to be a victim of a breach

- in the next twelve months?
  - 19%
  - 24%
  - 32%
- within twelve months to three years?
  - 23%
  - 24%
  - 26%
- in more than three years’ time?
  - 24%
  - 21%
  - 31%
- during a high profile commercial event (e.g. Black Friday, Amazon Prime Day, Christmas)
  - 22%
  - 21%
  - 31%
Impact of personal data being stolen

Two-thirds (66%) of surveyed consumers say that they would be unlikely to shop/do business with an organisation that experienced a breach where their financial and sensitive information was stolen.

Also, around three in ten (31%) would sever ties with a company if the consumers’ passwords were stolen.

This suggests that many consumers hold organisations accountable for protecting their personal information and will be unforgiving if the company cannot keep their details safeguarded.

Fig 11: Those that say they are unlikely for: “How likely would you be to shop or do business again with a company (retail, financial, healthcare) that had experienced a breach...”
Security measures in place

How seriously organisations take data protection

Only around three in ten (29%) respondents think that companies take the protection and security of customer data very seriously.

Moreover, a similar proportion (35%) of employed respondents report that their employer takes data protection of their data very seriously.

This suggests that most consumers have some doubts over organisations’ approaches when it comes to securing data for individuals – this explains why some consumers blame the organisation breached, if they have their personal information stolen.

<table>
<thead>
<tr>
<th>Very seriously</th>
<th>Fairly seriously</th>
<th>Not very seriously</th>
<th>Not at all seriously</th>
<th>I don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>50%</td>
<td>16%</td>
<td>2%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Fig 12: How seriously do you feel companies take the protection and security of customer data?

<table>
<thead>
<tr>
<th>Very seriously</th>
<th>Fairly seriously</th>
<th>Not very seriously</th>
<th>Not at all seriously</th>
<th>I don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>35%</td>
<td>41%</td>
<td>12%</td>
<td>2%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Fig 13: How seriously do you feel your employer takes the protection and security of employee data?
Who is responsible for securing personal data?

Respondents are much more likely to say that companies are responsible for protecting and securing customer data than customers are – 69.64% of responsibility falls onto the company vs. 30.36% on the consumer, on average.

This is likely to be linked to the fact that the majority of consumers do not believe that companies take the protection of their personal data very seriously, either as a customer (figure 12) or as an employee (figure 13).
Security measures for online/mobile banking

Over eight in ten respondents who use online or mobile banking report that passwords are a security feature in place (84% and 82% respectively).

Although organisations are using a range of security methods to protect data, they are often not using the advanced methods.

Fewer report that two-factor authentication is used for online (43%) or mobile (42%) banking, and only 15% say that biometrics is a security measure used for mobile banking.

---

**Fig 15:** Which of the following types of security are in place for your online banking?

- **Passwords:** 84%
- **Transaction security:** 50%
- **Two-factor authentication:** 43%
- **Encryption:** 31%
- **Fraud and risk management:** 23%
- **Biometrics:** 9%
- **Don’t know:** 5%

**Fig 16:** Which of the following types of security are in place for your mobile banking?

- **Passwords:** 82%
- **Transaction security:** 48%
- **Two-factor authentication:** 42%
- **Encryption:** 27%
- **Fraud and risk management:** 24%
- **Biometrics:** 15%
- **Don’t know:** 5%
Two-factor authentication for retail and social media sites

Although 69% of those surveyed that actively use online retail accounts say these accounts require two-factor authentication, only 25% claim that they all do.

A similar proportion (21%) of respondents that actively use social media say that all social media accounts use two-factor authentication.

This suggests that while many retailers and social media sites will use two-factor authentication to secure data, there are many more than do not.
Consumers’ engagement with security

Despite many surveyed consumers believing that companies could take the protection of customer data more seriously (figure 12), only the minority (28%) have provided feedback to organisations about their security methods.

Organisations may think that they have adequate security in place and that their customers are happy with the measures, but most consumers will not be informing them either way – potentially leaving companies unaware of dissatisfaction.

As it stands, only 16% of respondents claim to have a complete understanding of encryption with a similar proportion (13%) admitting that they have no understanding.

Most consumers do not fully understand encryption and therefore need organisations to feedback/educate their customers on their security method. However, customers rarely engage with organisations about security.

---

**Fig 19:** Have you ever provided organisations with feedback on what security methods they are offering/using?

- Yes, all the time: 6%
- Yes, occasionally: 12%
- Yes, once or twice: 9%
- No, but I have considered it: 19%
- No, I have not considered it but I might in the future: 40%
- No, and I have never considered it and never will: 15%

**Fig 20:** What level of understanding do you have regarding encryption?

- Complete understanding, I know exactly what it is and does: 16%
- Some understanding, I could know more: 44%
- Limited understanding: 28%
- No understanding: 13%
Online shopping and high profile events

Shopping online versus in-store

Respondents are more likely to do their shopping generally in-store (60.24%), on average but that leaves 39.76% the rest that is conducted online.

During a high profile commercial event (such as Black Friday), online shopping rises to 41.57%, on average.

Albeit most shopping takes place in-store, consumers are still conducting a large amount of shopping online, and during high profile commercial events this increases.

Fig 21: How much of your shopping do you do online compared to in-store generally, and how much will you do during a high profile commercial event (e.g. Black Friday, Amazon Prime Day and Christmas
Shopping online versus in-store

Respondents are more likely to do their shopping generally in-store (60.24%), on average but that leaves 39.76% the rest that is conducted online.

During a high profile commercial event (such as Black Friday), online shopping rises to 41.57%, on average.

Albeit most shopping takes place in-store, consumers are still conducting a large amount of shopping online, and during high profile commercial events this increases.

Consumers have clearly made the decision that they are prepared to take risks when it comes to their security, but should anything go wrong they put the blame with the business. The modern-day consumer is all about convenience and they expect businesses to provide this, while also keeping their data safe. With the impending threats of consumers taking legal action against companies, an education process is clearly needed to show consumers the steps they are taking to protect their data. Implementing and educating about advanced protocols like two-factor authentication and encryption solutions, should show consumers that the protection of their personal data is being taken very seriously.
Demographics

9,000 consumers were interviewed in September and October 2016. To qualify, consumers have to actively use online/mobile banking, social media accounts or online retail accounts.

### Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>2000</td>
</tr>
<tr>
<td>UK</td>
<td>1000</td>
</tr>
<tr>
<td>France</td>
<td>1000</td>
</tr>
<tr>
<td>Germany</td>
<td>1000</td>
</tr>
<tr>
<td>Russia</td>
<td>1000</td>
</tr>
<tr>
<td>India</td>
<td>1000</td>
</tr>
<tr>
<td>Benelux</td>
<td>500</td>
</tr>
<tr>
<td>Japan</td>
<td>500</td>
</tr>
<tr>
<td>Australia</td>
<td>500</td>
</tr>
<tr>
<td>UAE</td>
<td>250</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>250</td>
</tr>
</tbody>
</table>

### Age

- 18-24 years old: 1189
- 25-34 years old: 1492
- 35-44 years old: 1565
- 45-54 years old: 1567
- 55-64 years old: 1574
- 65 years and above: 1591
- Prefer not to say: 22

### Gender

- Male: 4495
- Female: 10
- Prefer not to say: 10
- 18-24 years old: 1189
- 25-34 years old: 1492
- 35-44 years old: 1565
- 45-54 years old: 1567
- 55-64 years old: 1574
- 65 years and above: 1591
- Prefer not to say: 22
ABOUT GEMALTO ENTERPRISE SECURITY

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.