Navigating Cyber Risks: Smooth Seas or Stormy Skies Ahead?
About the survey

The research was carried out by Amárach as part of an omnibus survey. The total sample for this survey was 1,000 people and the interviewing fieldwork dates were 12 to 16 October 2015.

Due to rounding, responses to the questions covered in this report may not aggregate to 100.
Welcome to our Deloitte Cybersecurity Review.

In this report we focus on personal data security and the challenges that cybercrime poses for consumers and consumer businesses.

We live in a digital economy. Social media, the Internet of Things, e-commerce and contactless payments are among the trends contributing to exponential growth in the volume and diversity of consumer data.

Businesses are amassing more personal information about their customers than ever before. This data is valuable to cyber criminals with the result that businesses are exposed to greater cyber risks than ever before. Stories of organisations getting hacked have become so frequent that it is easy to believe there’s no real way to avoid being the next target.

While consumers are alert to these dangers, they are distrustful of how organisations protect and use their personal information. Deloitte research shows that consumers want more control over their data privacy and would like businesses to provide them with better tools to protect themselves online.

Businesses can begin to address the trust gap by being more transparent about the information they collect and reassuring consumers about how their personal data is protected.

We hope this report gives you an insight into the opportunities for your business and we welcome your feedback.

If you would like further information on the survey please contact:

David Hearn
Lead Consumer Business Partner
T: +353 1 417 2535
E: dhearn@deloitte.ie
In the digital economy, businesses collect, store and analyse more information about consumers from more data sources than ever before. While access to real time information affords the opportunity to improve business decision making and increase profitability, this does not come without risks. Cybercrime is a real and growing threat. Stories of business websites being taken down and hacked are reported almost every day. The financial and reputational impact of attacks is often significant. Businesses need to proactively monitor their online reputation and be vigilant about spotting and reacting to indications of potential problems.

The latest Deloitte research shows that almost half of all consumers say that if their bank details were lost or hacked in a cybercrime attack on a business, they would never shop online or in-store with that business again.

The research also shows that consumers do not understand how to control the level of data available about them online and are distrustful of how businesses use their personal information. Consumers want more control over how their data is secured and would like businesses to provide them with more and better tools to protect their privacy online.

To address the trust gap, businesses need to become more transparent with their data protection processes, educating consumers about how their data is used and explaining the benefits of allowing data to be shared.
Key observations

1 in 10 consumers feel comfortable browsing, making payments and entering their card details using public WiFi.

3 in 10 consumers (29%) believe their mobile device is as secure as their laptop.

5 in 10 (52%) consumers feel comfortable checking their bank balance on a mobile device.

5 in 10 (47%-49%) of customers would no longer shop instore or online with a particular company if there was a data breach concerning their bank details.
Whether they purchase online or in-store, Irish consumers are savvy shoppers. 6 in 10 browse online before making an in-store purchase and almost half (48 percent) conduct "extensive online research" before they buy.

Most of this research takes place at home where consumers feel more secure online. There are low levels of trust in public and in-store Wi-Fi networks.

More consumers (55 percent) are paying their bills online, albeit sometimes because no other payment option is available.

Just under half (48 percent) of consumers claim they “often” buy goods on the internet while fewer than 1 in 10 “never” make online purchases.

Consumers’ attitude to public and in-store Wi-Fi shows that they are alert to the risks of cybercrime and concerned about the privacy of their personal information. This is both an opportunity and a challenge for consumer businesses. On the one hand, businesses can gain a competitive advantage by reassuring consumers about how their personal data is collected, stored and used. On the other hand, the more information that businesses collect, the more attractive that data becomes to cybercriminals, increasing the risk that the business may be subject to a cyber attack.
Consumers understand the dangers of sharing data on insecure networks and feel most comfortable when browsing and carrying out transactions on their home Wi-Fi network. There are low levels of trust in public and in-store Wi-Fi when it comes to entering payment details with fewer than 1 in 10 consumers comfortable making payments - or even browsing - on public networks.
According to the latest Deloitte research, 37 percent of Irish consumers feel comfortable browsing on mobile networks.

Just over half (52 percent) of consumers check their bank balance on mobile devices and 41 percent would transfer money on a mobile device.

Mobile networks are more trusted than public and in-store Wi-Fi both for browsing and completing transactions. In-store, consumers use mobile devices to compare prices and check online reviews. While relatively few consumers currently make transactions on their mobile devices—perhaps because entering the data required to complete a transaction (name, address and credit card number) can be cumbersome—this is likely to change as more businesses adopt mobile payment technologies.

Those who already use touch and go credit card payments are likely to avail of the convenience of replacing the card with their mobile phone and this is likely to result in an increase in mobile transactions.
The security of their personal data is very important to consumers, 76% of whom feel that businesses should be held responsible for protecting their customers' information online.

Consumers also feel that businesses should provide them with tools to protect their online privacy and they would like businesses to make more use of identification and authorisation processes to increase security on their websites.

Unless they have given express permission, consumers do not want businesses to share their personal data with third parties.

Clearly consumers would like businesses to take the lead in keeping them safe from cybercriminals. Businesses can turn this to their advantage by collaborating with their industry peers and government to counter cyber attacks and by integrating cybersecurity into their enterprise risk management systems while proactively reassuring consumers that their data is held securely.

Figure 4: Security of personal data

Security of personal data - 1

Companies need to be held responsible for ensuring the security of user data and personal information online

I expect companies that collect or process personal details or financial transactions online to keep this data secure from criminals

I expect companies that collect or process personal details or financial transactions online to refrain from sharing this data with third parties unless they request my permission to do otherwise

I think it is the responsibility of companies to provide me with the tools I need to protect my privacy, security and reputation online

I want companies to introduce more identification authorisation processes on their websites, such as security questions or using a pin code, despite the additional burden for me

I often think about the safety of my personal information online

Strongly agree
Agree
Neither/nor
Disagree
Strongly disagree
Don’t know/not applicable

The security of their personal data is very important to consumers, 76% of whom feel that businesses should be held responsible for protecting their customers' information online.

Consumers also feel that businesses should provide them with tools to protect their online privacy and they would like businesses to make more use of identification and authorisation processes to increase security on their websites.

Unless they have given express permission, consumers do not want businesses to share their personal data with third parties.

Clearly consumers would like businesses to take the lead in keeping them safe from cybercriminals. Businesses can turn this to their advantage by collaborating with their industry peers and government to counter cyber attacks and by integrating cybersecurity into their enterprise risk management systems while proactively reassuring consumers that their data is held securely.
I often think of the need for me to protect my activities and data online.

My bank is responsible for protecting me from payment or credit card fraud online.

The government should be responsible for enforcing online data protection and personal security.

I am concerned about the security of my personal data when paying for goods and services online.

It is my responsibility to take control of my digital presence and ensure that my personal information is safe online.

I am confident that I have up-to-date security software in place on my digital devices (such as a computer or Smartphone) to protect me while being online, browsing, or sharing data and information.

While consumers worry about security when purchasing goods and services on the Internet, just over half (58 percent) are confident that they have up-to-date security software on the devices they use when browsing and sharing information online.

Although they acknowledge their personal responsibility for protecting their own data online, consumers rely on banks to keep them safe from online payment and credit card fraud and expect government to enforce data protection.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
<th>Don’t know/not applicable</th>
<th>Neither/nor</th>
</tr>
</thead>
<tbody>
<tr>
<td>I often think of the need for me to protect my activities and data online</td>
<td>6</td>
<td>44</td>
<td>21</td>
<td>24</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>My bank is responsible for protecting me from payment or credit card fraud online</td>
<td>7</td>
<td>33</td>
<td>31</td>
<td>25</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>The government should be responsible for enforcing online data protection and personal security</td>
<td>5</td>
<td>39</td>
<td>24</td>
<td>28</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>I am concerned about the security of my personal data when paying for goods and services online</td>
<td>7</td>
<td>44</td>
<td>19</td>
<td>27</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>It is my responsibility to take control of my digital presence and ensure that my personal information is safe online</td>
<td>4</td>
<td>47</td>
<td>16</td>
<td>30</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>I am confident that I have up-to-date security software in place on my digital devices (such as a computer or Smartphone) to protect me while being online, browsing, or sharing data and information</td>
<td>8</td>
<td>44</td>
<td>14</td>
<td>29</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Despite their concerns about online privacy, just over half (53 percent) of consumers control their privacy settings and only 42 percent understand how to control the level of data or information available about them.

Consumers would like businesses to use more authorisation and identification tools to protect them from cybercrime. Businesses responding to this demand, however, need to ensure that authentication is intuitive and seamless so as to maintain the balance between security and usability. Passwords, encryption, two-factor authentication or one time passwords where a code is sent to a consumer’s mobile phone or other digital device to verify the user’s identity, are among the most commonly used authorisation and authentication tools.

Consumers also worry about the security of their personal data when they are physically paying for goods and services in public locations such as stores, hotels and restaurants. In future, it is likely that technologies such as biometrics and near field communications (NFC) will replace card and pin transactions making mobile payments in these situations more seamless and potentially more secure.

At the moment, however, only 29 percent of Irish consumers feel their mobile phone is as secure as their laptop. A significant 38 percent consider that mobile devices are less secure.
Trust and transparency

Reports of data breaches and cyberattacks make consumers distrustful about how their personal data is secured and used.

Consumers want businesses to be held responsible for ensuring the security of user data and personal information. They also want greater control over their personal data and would like businesses to provide them with tools to protect themselves online.

Businesses prepared to respond to these demands stand to benefit from a loyalty dividend since customers engaged under the principles of transparency, clarity and data security are more likely to stay.

Businesses can also win consumer confidence by using features such as verified purchase reviews or putting payments through an established third party payment processor however they must explain the benefits of these processes to their customers in order to build trust.
Security breaches

Stories of businesses being targeted by cybercriminals are becoming more frequent and the impact of attacks can be lasting.

Deloitte research shows that if their bank details were compromised in a cyber attack on a store, almost 50 percent of Irish consumers would cease business with that store altogether.

International costs for a breach are currently quoted as approximately €150 per record. However there are intangible costs that are hard to quantify such as loss of current and new customer confidence. In some industries there is no going back from a breach of trust.

<table>
<thead>
<tr>
<th>Event Description</th>
<th>10</th>
<th>19</th>
<th>38</th>
<th>21</th>
<th>12</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A website crash resulting in website being offline for less than an hour</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A website crash resulting in the website being offline for less than a day but more than an hour</td>
<td></td>
<td></td>
<td>37</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A data breach where customer's personal details such as names and addresses were lost/hacked</td>
<td></td>
<td>36</td>
<td></td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A data breach where payment details such as bank details were lost/hacked</td>
<td></td>
<td></td>
<td>47</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reaction to the event</th>
<th>78</th>
<th>19</th>
<th>38</th>
<th>21</th>
<th>12</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>I would wait until the issue was resolved before completing any online or in store purchases</td>
<td>10</td>
<td>28</td>
<td>37</td>
<td>23</td>
<td>17</td>
<td>8</td>
</tr>
<tr>
<td>I would wait until the issue was resolved before completing any online purchases</td>
<td></td>
<td></td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I would never shop from them online or in store</td>
<td>11</td>
<td>19</td>
<td>36</td>
<td>21</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>I would shop in their physical store only</td>
<td></td>
<td></td>
<td>38</td>
<td>21</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>I would not affect my shopping habits in any way</td>
<td>4</td>
<td>4</td>
<td>26</td>
<td>16</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Figure 7: Security breaches
Security scares and purchasing behaviours for - loyal customers
For most businesses, it’s no longer a question of ‘if’ they suffer a cyber attack, but rather ‘when’. Some of the more disruptive and damaging events that we are seeing in Ireland at the moment are banking Trojans, ransomware, DDoS (Distributed Denial of Service) and fund diversion by social engineering.

A scam that several Irish organisations have been exposed to in recent months involves a series of spoofed emails, invoices, letters or calls requesting that funds be transferred to an illegitimate bank account.

When developing a cybersecurity strategy, it is important that businesses understand the data they hold and protect their information assets in direct proportion to what makes them attractive, to whom and the impact that losing them might have on the business.

Figure 8: Security breaches
Security scares and purchasing behaviours for - when just browsing with a company

- A website crash resulting in website being offline for less than an hour
  - 14%

- A website crash resulting in the website being offline for less than a day but more than an hour
  - 23%

- A data breach where customers personal details such as names and addresses were lost/hacked
  - 41%

- A data breach where payment details such as bank details were lost/hacked
  - 49%

- I would wait until the issue was resolved before completing any online or in store purchases
  - 13%

- I would shop in their physical store only
  - 25%

- I would wait until the issue was resolved before completing any online purchases
  - 10%

- I would not affect my shopping habits in any way
  - 7%
An integrated approach to cybersecurity

Change in the regulatory environment and implications

The European Commission is in the process of overhauling EU data protection legislation with the proposed introduction of regulatory requirements that are likely to impact businesses across all sectors. While the reform is focused on improving consumer protection, current proposals seem likely to result in extra burdens and restrictions for businesses.

With the rules set to change, businesses are likely to face a variety of new technical and procedural challenges. If businesses fail to act early they could struggle to align policies and procedures with the new requirements. This could result in fines for non-compliance, reputational damage or missed opportunities to demonstrate to customers that the business treats their data responsibly.

From 2018, businesses operating in Ireland will need to meet these new standards.

Proposed changes and potential impact:

<table>
<thead>
<tr>
<th>Proposed requirement</th>
<th>Description</th>
<th>Potential impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to data portability</td>
<td>Where personal data are processed by electronic means and in a structured and ‘commonly used’ format, they must be provided to an individual in a ‘commonly used’ format upon request.</td>
<td>• Impacts across all business units, including data processors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Divergent, highly segregated systems are unlikely to be compliant.</td>
</tr>
<tr>
<td>Breach notification</td>
<td>Notification of a data breach to the supervisory authority and to the data subject within a specified timeframe.</td>
<td>• Impacts across all business units, including third parties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Incident management procedures will need to be updated.</td>
</tr>
<tr>
<td>Transparency</td>
<td>Policies relating to data protection should be transparent and easily accessible.</td>
<td>• Impacts data capture forms across a variety of on and offline media platforms.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Privacy policies will need to be updated.</td>
</tr>
<tr>
<td>Privacy by design</td>
<td>If a processing operation presents a specific risk to the rights and freedoms of individuals, the controller must carry out auditable Privacy Impact Assessments.</td>
<td>• Impacts project development lifecycle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tools and templates will be required to conduct impact assessments.</td>
</tr>
<tr>
<td>Consent</td>
<td>Consent must be unambiguous and may require opt-in from individuals.</td>
<td>• May need to assess and update consent mechanisms across a wide variety of communication channels.</td>
</tr>
<tr>
<td>Right to erasure</td>
<td>Requires organisations that hold personal data to erase data relating to an individual and to stop further dissemination of such data, upon receipt of a request.</td>
<td>• Significant effort required to locate and delete personal data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Issues with partial or incompatible data sets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Practical difficulties with information processed by third parties.</td>
</tr>
</tbody>
</table>
As the frequency of cyber attacks increases, businesses are becoming aware that cybersecurity is not just an IT or technology issue but impacts all aspects of the organisation. Monitoring risks and implementing controls that are integrated with other risk management processes across the organisation is the best way to protect against cyber attacks.

Data audit
The first step in protecting a business is to map its data assets and confirm that the business is complying with its legal, data protection and consumer obligations. What data is collected, by whom, when and for what purpose? Where is the data stored? How is the data updated? It is important to understand the nature, complexity and volume of data in order to prioritise risks and protect against them accordingly.

Risk identification
The next step is to identify breach scenarios and assess their likely impact on the business. It is important that businesses obtain an independent view of the potential risks as they may otherwise have an inaccurate or incomplete view of their vulnerabilities.

Build trust
There is value in building trust with consumers by explaining how and why their personal information is collected and secured. Businesses need to allow consumers control over how their personal data is used and should implement authentication tools to afford consumers greater confidence that their transactions are protected.

Monitor reputation
Phishing, fraudulent websites, fake branded goods all have the potential to damage a business. Businesses should be vigilant about monitoring their online reputation, taking down fraudulent websites, reporting phishing, gathering intelligence about the types of attacks and investigating suspicious activities.

Response plan
Businesses need to plan for the worst and develop the capability to forensically investigate cyber attacks so that the extent of any damage can be quickly identified and repaired. Incident response plans should be prepared and tested while a communications plan should be developed to minimise the reputational impact of an attack. Businesses should also consider purchasing services or insurance to protect against common cyber attacks such as DDoS and their impact.

With appropriate planning, systems, technologies and monitoring, many cyber attacks can be prevented and the impact of attacks, when they do occur, can be mitigated.
Contacts

For more details please contact:

**Dublin**
Deloitte
Deloitte & Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

**Cork**
Deloitte
No.6 Lapp’s Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

**Limerick**
Deloitte
Deloitte & Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

**Galway**
Deloitte
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099
www.deloitte.com/ie

For more information on the Deloitte Consumer Review please contact:

**David Hearn**
Partner, Consulting
T: +353 1 417 2535
E: dhearn@deloitte.ie

**Jacky Fox**
Digital Forensic and Cyber Security Lead
T: +353 1 417 2208
E: jacfox@deloitte.ie

**Sinead McHugh**
Director, Audit
T: +353 1 417 2817
E: simchugh@deloitte.ie

**Colm McDonnell**
Partner, Risk Advisory
T: +353 1 417 2348
E: cmcdonnell@deloitte.ie

---

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As one of the largest global professional services and consulting networks, with over 220,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has approximately 2,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience, and insight to collaborate with clients so they can move forward with confidence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2016 Deloitte. All rights reserved