Online domain maturity

How to provide a superlative online experience for your customers

October 2014

Almost all businesses now interact online with their customers; they have no choice if they want to remain competitive. However, there is a choice as to how well online customers are served. Those businesses that transact directly with the fickle and capricious consumer market have adapted faster in making sure their online presence is at the cutting edge.

This consumer-facing majority give more attention to their online domains than the non-consumer-facing minority that only have business-to-business dealings. This report identifies seven areas where this is the case, leading to better monitoring, management and security capabilities; a higher overall domain maturity. Achieving this is partly down to investment but also outsourcing the basics, freeing them to focus on business issues rather than technology ones.

The report presents new research into how European organisations are using and managing their online domains, the challenges they face and how these are being overcome. It should be of interest to anyone with responsibility for maintaining their organisation's ability to transact online with its customers.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: +44 7711 719505
Email: Clive.Longbottom@Quocirca.com

Executive Summary

Online domain maturity

How to provide a superlative online experience for your customers

The overwhelming majority of organisations now transact online with their customers at some level. However, those that have to deal with the fickle and capricious nature of consumers have adapted fastest, putting in place the tools that ensure the performance and security of online services. Many of them find that outsourcing whole web sites or applications, or at least some of the management responsibilities, is the fastest route to reach advanced domain maturity.

For many organisations, their online domain is now their kingdom

Almost all European organisations (98% plus) now transact online at some level. This means that, for many, their online domain is now one of their most important assets. The volume of registered users may run into hundreds of thousands, or even millions for larger businesses. This now means that taking measures to protect domain performance and security have become a top priority; however, some have travelled this road further than others.

Those with B2C dealings have had to rise to the challenge fastest

Just over 77% of all European organisations transact online with consumers (B2C), usually alongside dealings with other businesses (B2B). The remainder only deal with other businesses (B2B only). At all levels, the differences between these ***consumer-facing*** and ***non-consumer-facing*** organisations are telling, including the degree of investment in their online domains, the tools they put in place, their view of outsourcing, and use of on-demand services. In short, consumer-facing organisations have a higher ***domain maturity***.

Online priorities include web sites, applications and supporting services

Consumer-facing organisations place a higher priority on nearly all forms of online resources. Obviously, this includes their website and online applications, which are the front line for transacting with customers. However, it also includes supporting services such as online payments and CRM. They also recognise the need to interface with social media providers to help drive consumers to their primary services. As consumer-facing organisations become dependent on their own online domains, they find it easier to trust such services from others.

Concerns about the impact of poor domain performance vary

All organisations worry about the user experience being degraded if the online domain is impacted in some way. However, consumer-facing organisations are more likely to have overcome many basic performance and security issues and this frees them to focus instead on those that affect the bottom line, such as attracting new customers and maintaining competitive edge in general.

Consumer-facing organisations invest more in their domains

Consumer-facing organisations are more likely to dedicate budget to protecting their domains. This enables them to invest more, for example in tools to measure the user experience and carry out customer-related analytics. Non-consumer-facing organisations are more likely to be bogged down with basic network issues and using out-of-date security technology. This is partly due to lack of funds but also because they are reticent to outsource.

Outsourcing should be seen as a solution rather than a risk

Whether it is outsourcing a web site or online application in its entirety or just elements of it, consumer-facing organisations are more likely to have done so. This includes the management and protection of DNS infrastructure, content distribution and security services including DDoS protection, advance threat protection, and security information and event management (SIEM). Trusting such issues to third parties frees up resources to focus on what really matters, generating business online.

Conclusions

Transacting with customers online is no longer a choice but a necessity. The battle for any business is to do it better than others. This competition is at its most fierce when it comes to winning over consumers. To this end consumer-facing organisations have matured their online presence more so than their non-consumer-facing counterparts. That said, in many areas, including monitoring and measuring online activity, all have room for improvement. There is still plenty of scope to get ahead in the race to have the best performing online domains.

Your kingdom is your domain

When a new business is created, much thought goes into what it should be called. Even before the internet became a shop window and trade floor for the majority of businesses, choosing a company name could be problematic; was it already registered somewhere? was it copyrighted? Today, there is also the need to obtain the rights to online domain names that exactly or closely match the company name.

For organisations with global aspirations, despite all the new domain extensions (.city, .bio, .market etc.), only .com will do. Others may want their domain to appear more local, .fr, .de, .co.uk and so on. Once settled on, the reputation of an organisation's online domain will form an essential part of its overall reputation. If web sites or online applications perform poorly, or their security is compromised, the domain reputation and, therefore, overall brand, suffers.

This report presents new research into what motivates European organisations to protect their online domains, what problems they have in doing so, and the measures they are taking to ensure domain performance and security. For the majority, the internet is now essential to transacting with consumers and other businesses. For some it is everything, the full extent of their kingdom that needs protecting at all costs. Too many are still not doing this adequately.

B2B and/or B2C

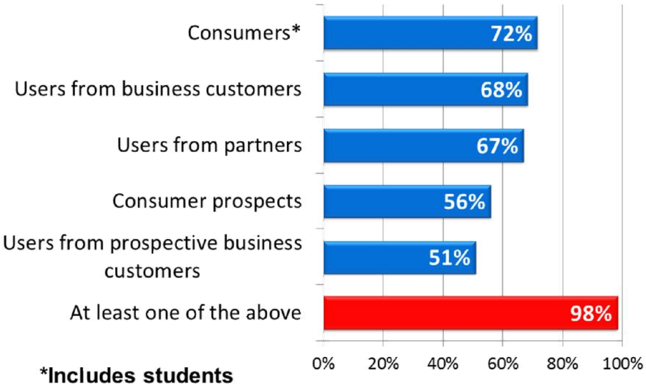
Historically, many IT applications were designed to support internal users; with websites and online applications it is primarily about outsiders. Over 98% of European organisations now deal online with consumers, business customers or partners (Figure 1).

There is much overlap; many organisations having online dealings with consumers, other businesses and partners. However, if partners and business relationships are considered together as business-to-business (B2B), the data can be simplified and any organisation considered as either consumer-facing or non-consumer facing (Figure 2).

As the analysis presented in this report shows, consumer-facing businesses face up to the challenges of online life better than non-consumer-facing ones, even though the latter nearly all have to manage online B2B relationships anyway. Why should this be so?

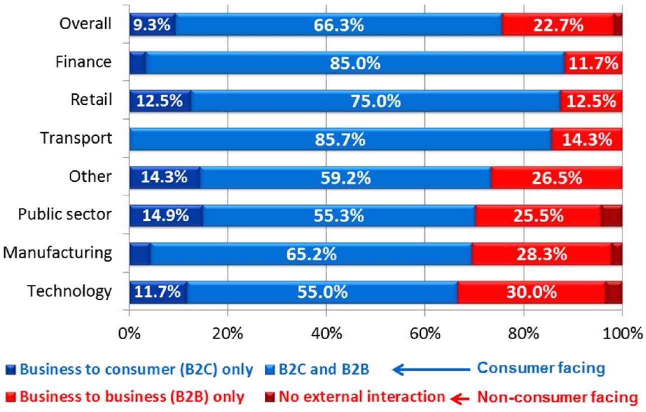
To start with, one business may tolerate faults in another business's online service, recognising the challenges involved. In addition, a business user sitting waiting for a response is often doing so as part of their job and not proactively choosing the online services they deal with. As business users they will generally be more tolerant than they would be as consumers.

Figure 1: Types of external users regularly interacted with online (overall)



***Includes students**

Figure 2: External interaction by industry sector



Consumer relationships are more fragile and ephemeral. The effort of luring a consumer to a site is wasted if the frustration of waiting for a response leads them to abandon and go elsewhere. Security is an issue too; incidents may affect reputation and B2C interactions tend to be more regulated than B2B ones; for example taking online payments, which can bring an organisation into scope for PCI DSS (the Payment Card Industry Data Security Standard).

The reach provided by the internet is democratising; smaller businesses are as likely to be consumer-facing as larger ones. However, unsurprisingly, size does make a difference in one area: the number of individuals that an organisation has a relationship with that requires them to register for an online service in some way (Figure 3). Figure 3 also shows that consumer-facing businesses deal with far more registered users than their non-consumer-facing counterparts. Another driver that has led them to invest more in their online domains is the need for scalability.

Within different industry sectors, finance and transport are the heavy hitters when it comes to number of registered online users (Figure 4). Retailers tend to deal more in the thousands than millions, leaving them surprisingly low on the list, despite their strong tendency to be consumer-facing. This is why overall numbers alone do not serve as the best indicator of how important a given organisation's domain is to its business and the degree they are prepared to invest in its performance and security.

Figure 3: Number of individual registered external online users

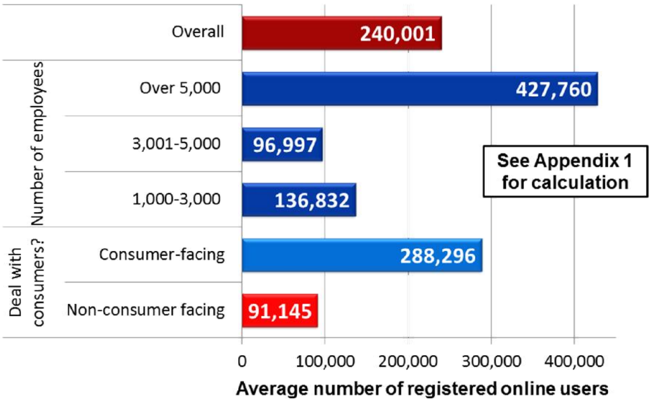
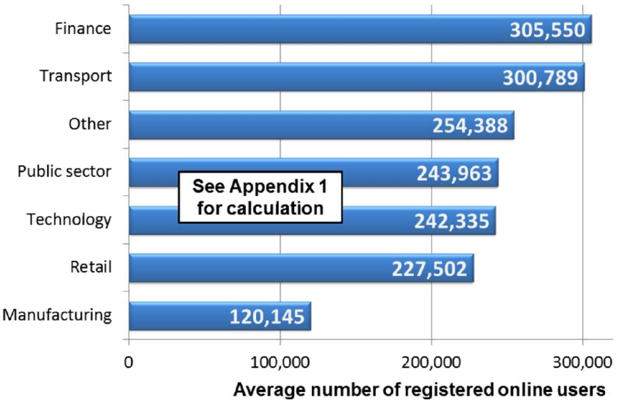


Figure 4: Number of individual registered external online users – by industry sector



Domain priorities and maturity

In all cases, consumer-facing organisations consider their online resources and certain supporting applications as more important than their non-consumer-facing counterparts (Figure 5); on average, all score higher than 3.5 out of 5 on a scale where 5 is ‘*very important*’. For all organisations, informational web sites top the list; these may be just shop windows but, for many, it will be their only or primary one, which they cannot afford to neglect. However, whether it is with consumers or other businesses, the majority now transact online either via their web site or purpose built applications, which will increasingly be designed for mobile use.

To facilitate online commerce, many invoke supporting applications and services. Figure 6 illustrates some wide gaps between consumer-facing and non-consumer-facing organisations. Consumer-facing organisations are much more likely to use payment systems, securing payment at the time an order is placed (bringing many into scope for PCI DSS). With B2B transactions, whilst an order may be placed online, credit lines may mean payments are made later via another channel. The value of social media is increasingly recognised for attracting consumer buyers, but less so for new business contacts.

Differences there may be, but what is not in doubt is that online activity is important for the majority of organisations and this makes the reputation and security of their domain a top level priority for business management, not just one for IT managers to fret about. This is reflected in the concerns shown should a domain fail to deliver in some way and no longer adequately serve business requirements. It is also reflected in the maturity of domain protection capabilities.

Figure 5: How important are the following online services for your business when interacting with external users?

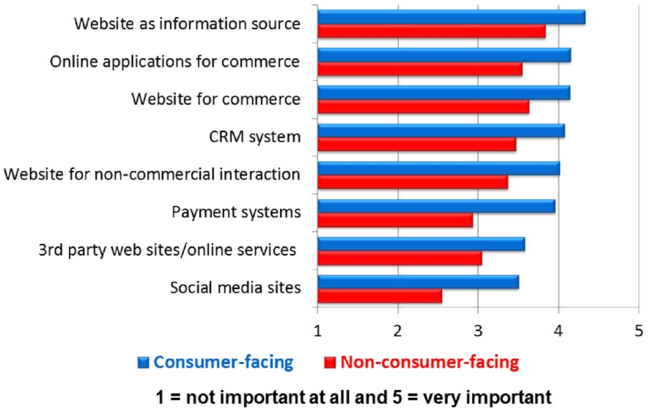
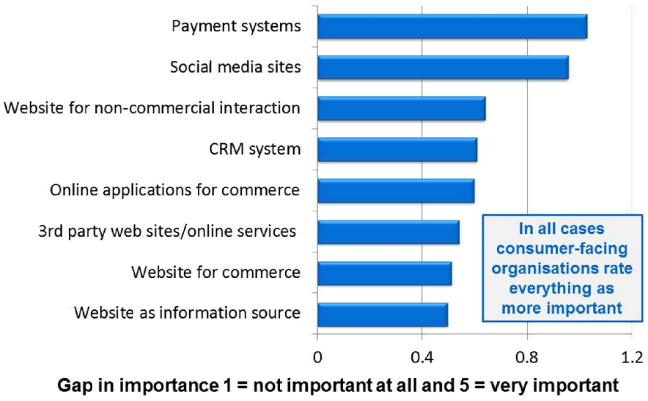


Figure 6: How important are the following online services for your business when interacting with external users?



In all cases consumer-facing organisations rate everything as more important

Concerns about domain performance and security

When it comes to the top priorities for ensuring online services are performing in line with business expectations, a more complex set of differences between consumer-facing and non-consumer-facing organisations emerge (Figures 7 and 8). No one wants a poor user experience or to suffer a security problem. However, such issues can be mitigated, which is the essence of domain maturity.

Consumer-facing organisations place commercial issues high on the list, such as attracting new customers or losing out to competitors. Non-consumer-facing organisations worry more about security and the reputational damage that may arise if their domain is compromised.

This ordering of priorities by consumer-facing organisations is not down to complacency. Figure 9 shows the rating of specific issues that may arise with regard to domain performance and security. All are a worry, scoring between 3 and 4 out of 5 where 5 is '*a big concern*'. In fact, in all areas consumer-facing organisations are a little more concerned. The difference is, as this report will go on to show, is that consumer-facing organisations are more likely to have taken measures to mitigate these, i.e. they have higher domain maturity. This frees them to focus on commercial priorities as just noted.

Figure 7: Top three concerns with regard to online services underperforming in some way

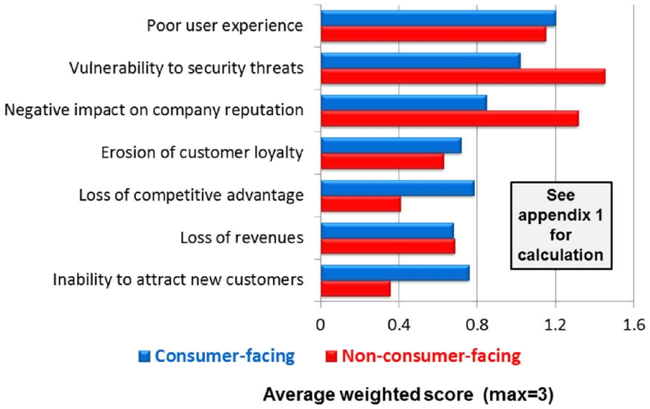


Figure 8: Top three concerns with regard to online services underperforming in some way

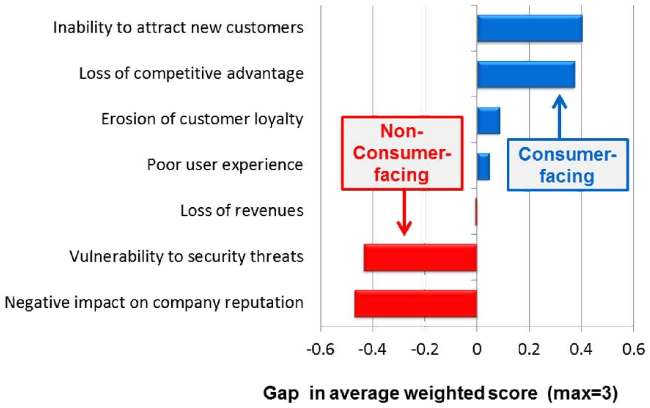
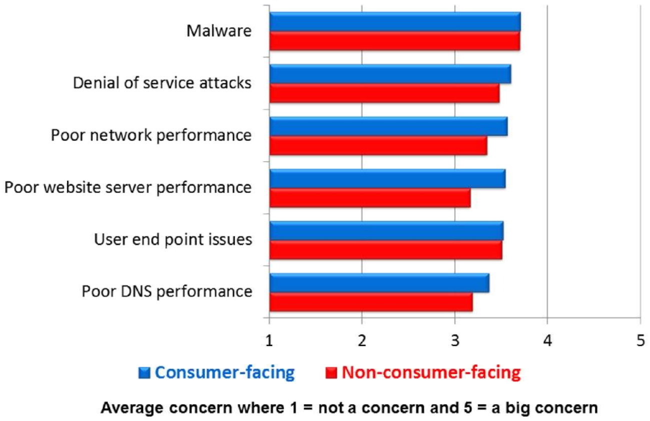


Figure 9: Concerns with regard to the performance and security of online services



Seven ways in which domain protection is ensured

There are a number of things that can be done to better protect online domains. Quocirca's research identified seven things that consumer-facing organisations, with their greater domain maturity, were more likely to be doing than their non-consumer-facing counterparts.

1 – Invest more

Being free to focus on commercial issues involves having other, more technical, controls in place in the first place. Of course, these are rarely free; the need for investment must be understood and funds made available. This is indeed the case. The first thing consumer-facing organisations are more likely to be doing is to have dedicated budgets for supporting online resources (Figure 10).

2 – Monitor performance

Furthermore, consumer-facing organisations spend this budget in different ways (Figure 11). Basic performance monitoring capabilities, such as variable load testing, are of equal priority for all. However, non-consumer-facing organisations tend to be bogged down with fairly technical issues, such as monitoring bandwidth and gathering system information. Consumer-facing organisations are more likely to spend their budget on the customer-related issues such as user experience monitoring (UEM) and integrating user data with web analytics (Figure 12), although less than 50% have invested so far.

3 – Take a granular approach

This goes hand-in-hand with a more sophisticated capability to measure the granularity of the user experience, based around issues such as user location, browser type, connect-speed, and user access device (Figure 13). However, whilst twice as many consumer-facing organisations have strong capability in these areas as non-consumer-facing ones, the majority admit there is room for improvement; only the most mature can do this well.

Figure 10: Dedicated budgets for supporting online resources – expected change during next year

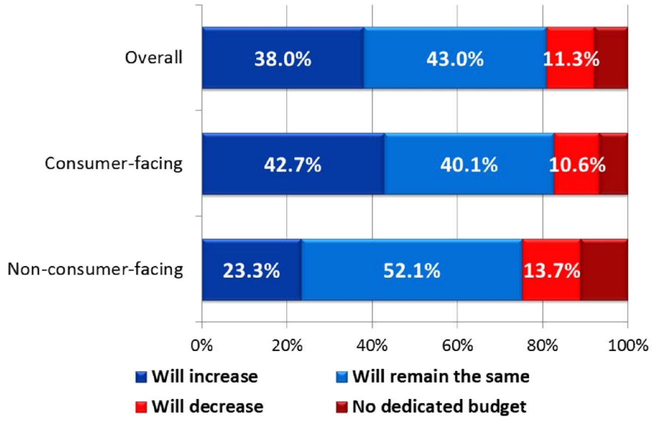


Figure 11: Capability to test, monitor and remediate problems with online services

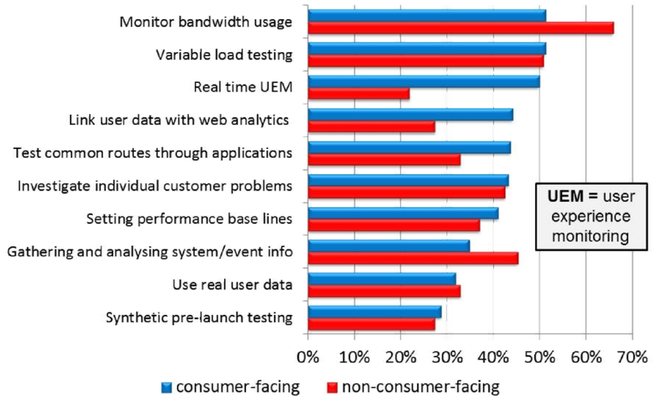


Figure 12: Capability to test, monitor and remediate problems with online services

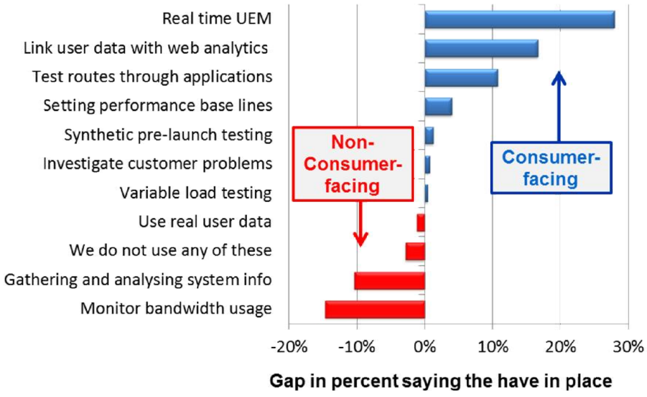
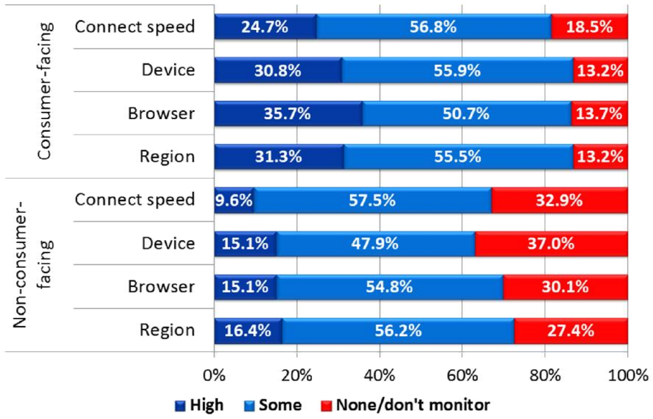


Figure 13: Granularity of monitoring of online services



4 – Put in place advanced security

Various security measures are much more likely to be in place across the board than those for performance monitoring. Many of these, such as DDoS and DNS infrastructure protection, are specific to domain protection and are high on the list of priorities (Figure 14).

In many areas there is a telling gap between consumer-facing and non-consumer-facing organisations (Figure 15). Exceptions are malware detection/blocking and intrusion detection systems (IDS). Host based malware defence is a last line of defence when others have been breached; for example, where advance threat intelligence is not in place or has not blocked malware from arriving in the first place. IDS, is an outdated technology that has largely been superseded. Many may still have legacy IDS systems as a line of defence, but the more mature consumer-facing organisations are more likely to also be protected by state-of-the-art technology.

Where domain infrastructure is managed largely on-premise, then some of these protections need to be alongside, which is the case. However, having access to the excess capacity to provide emergency protection, for example during a DDoS attack, only really makes sense as an on-demand service.

5 – Measure the user experience

When it comes to being able to measure the commercial impact of investment in domain performance and security, only a minority have strong capabilities (Figure 16). There is plenty of scope for improvement for all organisations. Zoning in on just 'strong capability' shows another telling gap between consumer-facing and non-consumer-facing organisations when it comes to '*understanding how user behaviour affects the bottom line*' and '*measuring customer loyalty in general*' (Figure 17).

Figure 14: Security capabilities in place for protecting and ensuring the availability of online services

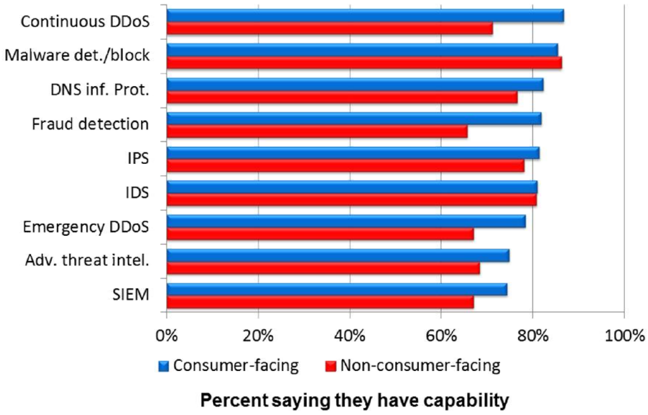


Figure 15: Security capabilities for protecting and ensuring the availability of online services

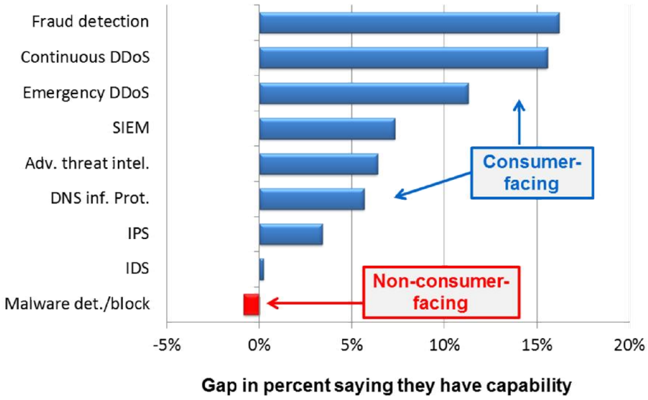


Figure 16: Capability to measure online services

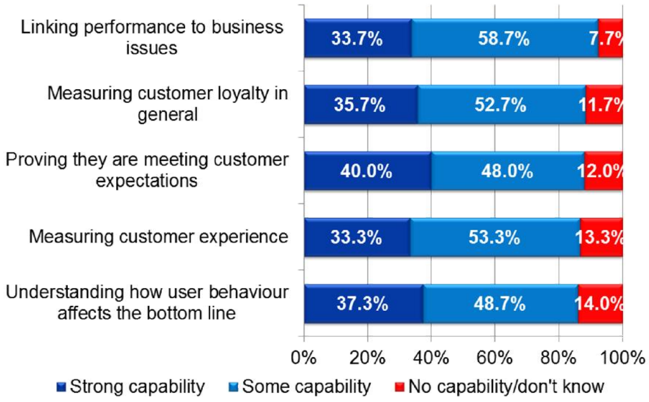
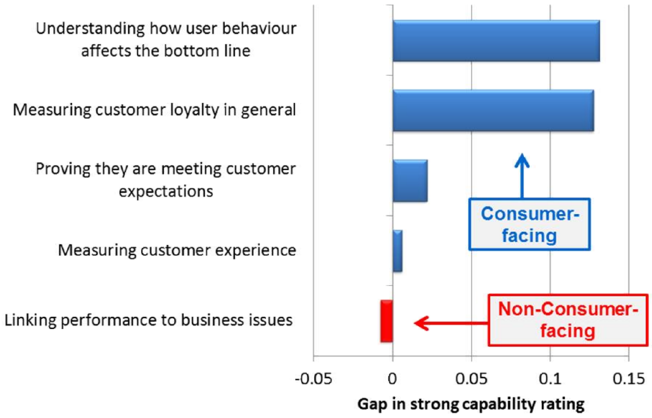


Figure 17: Capability to measure online services

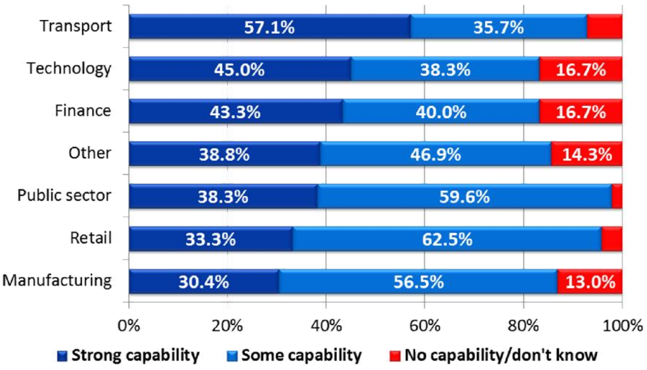


Understanding behaviour helps understand why potential transactions are not completed; maybe a user has become impatient or confused, or they may just have gone to check other options before returning to place an order. Having turned a visitor into a customer, enticing them back again should involve less effort, providing the new relationship has been cemented in some way, hence the need to measure customer loyalty. These two issues are of particular concern to consumer-facing organisations due to the fickle and capricious nature of consumers.[1]

It is important to note that in the five areas of domain performance measurement listed in Figure 16, overall only 40% or less have a '*strong capability*' in place, so the majority, consumer-facing or otherwise, can take a lead from the minority and strengthen their capability to be proactive in their ability to monitor domain performance and take actions to improve it.

Figure 18 singles out '*proving online services are meeting customer expectations*' by industry sector showing some stark differences. Only in transport do the majority have a '*strong capability*'; imagine the chaos on the Paris Metro, Berlin U-Bahn or London Underground if online services fail; the ability to travel is now often linked to online ticketing and payment systems.

Figure 18: Capability to measure online services



Sector ratings for "*Proving online services are meeting customer expectations*"

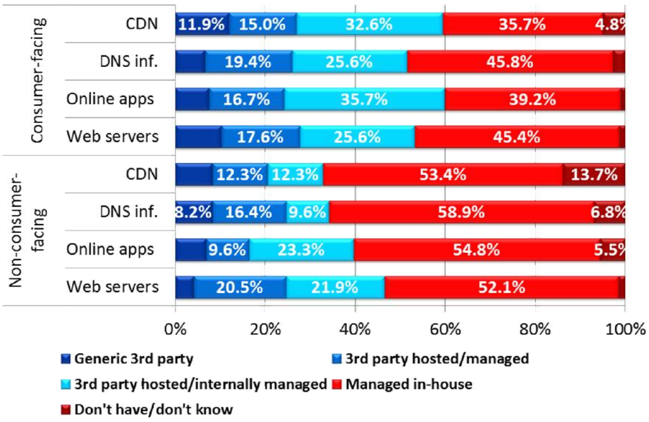
Technology organisations may be high on the list because of who they are; they are more likely to have the in-house skills to achieve these goals. However, a lack of in-house knowledge is no excuse for not improving domain maturity. In fact, trying to do so in-house is a distraction, which is why more and more organisations, especially consumer-facing ones, are outsourcing the hosting and management of their online services.

6 – Outsource infrastructure

As with any contemporary IT deployment, there are three choices for deployment of externally-facing online services; on-premise, fully hosted, or some hybrid mix of the two. The whole deployment of a website or online application can be outsourced and consumer-facing organisations are more likely to do this (Figure 19).

The evidence presented so far in this report suggests that this automatically improves their domain maturity and frees them up to focus on the business priorities related to delivering online services rather than technical ones. With hybrid deployments, where the online resource itself is hosted, but the end-user organisation is still involved, it is likely that this will be hands-on management of commercial issues rather than technical ones.

Figure 19: How are the following online services and supporting resources managed in your business?



CDN = content delivery network
DNS inf. = domain name service infrastructure

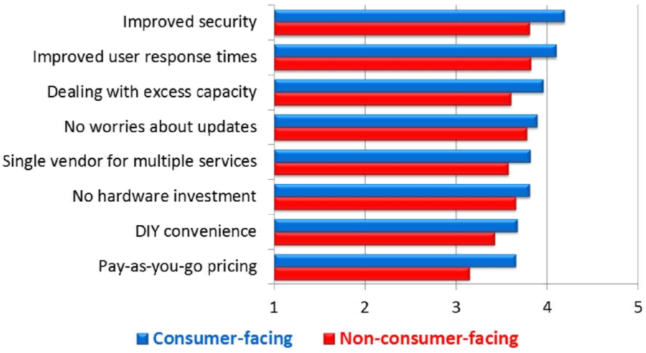
[1] NOTE: it also helps to get them to register an identity and/or create an account, which will be the subject of a forthcoming Quocirca report based on this research.

Beyond the online services themselves, consumer-facing organisations are more likely to entrust DNS infrastructure protection to a third party and to use a content delivery network (CDN). Indeed, saying content delivery is managed in-house is akin to saying it is not in place at all, as very few organisations will have the global points of presence (POPs) necessary to rival commercial CDN providers.

Most organisations recognise there are a range of benefits to be had from cloud-based services (Figure 20) and improved security tops the list. This is long overdue recognition that reputable cloud providers invest in and provide security measures that are beyond the means of individual organisations. A good example would be DNS infrastructure protection; it is far easier and more cost effective to share the cost of this across multiple customers than to put it in place on a case-by-case basis.

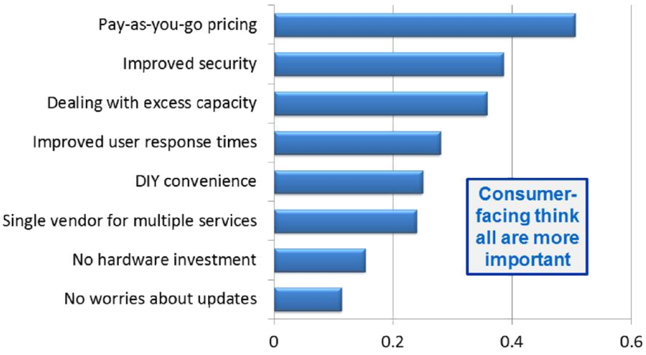
All the potential benefits of cloud based services listed in Figure 20 score more than 3 out of 5 where 5 equals '*very important*'. Whilst '*pay-as-you-go pricing*' is lowest on the list overall, it tops the list where the gap between non-consumer-facing and consumer-facing organisations are considered (Figure 21). Consumer visitor volumes are always likely to be more volatile than those of business customers; flexible pricing helps to deal with this.

Figure 20: How important are the following potential benefits of cloud-based services?



Average where 1 = not important at all and 5 = very important

Figure 21: How important are the following potential benefits of cloud-based services?

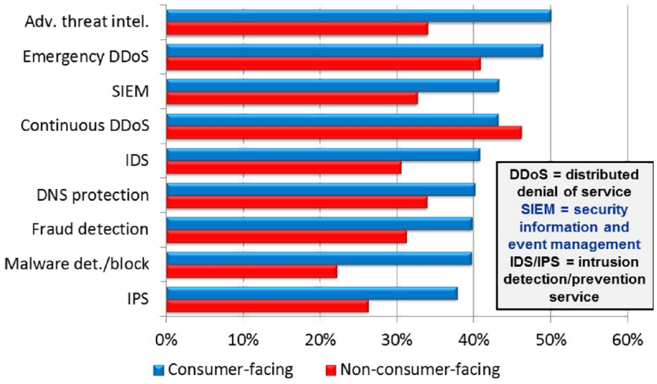


Gap in average importance, 1 = not important at all and 5 = very important

7 – Outsource security

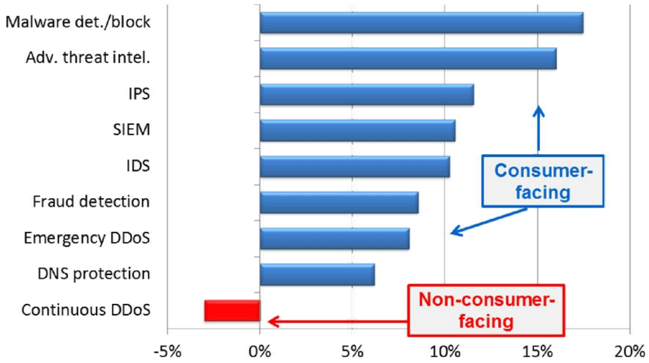
Many security services can also be procured as on-demand services; overall around 30% are doing so in one area or another (Figure 22). Again, consumer-facing organisations are more likely to use on-demand security, with non-consumer-facing organisations only taking the lead with continuous DDoS protection. This may well be because, with their greater tendency to outsource the management of on-demand services in the first place, consumer-facing organisations would consider such basic protection to be part of a service level agreement from their outsourcer and would not expect to pay for it separately. They have truly freed themselves to focus on business priorities rather than technology.

Figure 22: Use of on-demand security services



Percent saying they use on-demand service

Figure 23: Use of on-demand security services



Gap in percent saying they use on-demand service

Conclusion – the future of your domain

The internet is now embedded in business processes; the choice now is how well a given business manages its online presence rather than whether it has an online presence in the first place. Dealing with consumers raises the biggest challenge and consumer-facing organisations are rising to this, investing more in their online domains ensuring online security and performance.

That said, across the board, many organisations could learn from those making the most advanced use of certain tools such as those for measuring user experience and applying analytics to customer data. One reason some are failing to do this is because they are too involved in managing the technology platforms that support their online presence; they should free themselves from this burden. The best way to do so is either to outsource web sites and online applications in their entirety, or at least key aspects that ensure performance and security such as DNS infrastructure management, content distribution, and security requirements; for example DDoS defence.

The race to have a superlative online presence via a mature domain is one all businesses must join, whether they like it or not. The winners will be ready to face the future; the losers will not be part of it.

Appendix 1 - calculations

Calculation of transaction volumes

For the data used in Figures 3 and 4 the original question was put to respondents as follows:

What best represents the number of individual external users that your organisation has a relationship with that requires them to register in some way for access to certain online resources?

1. Tens (10s)
2. Hundreds (100s)
3. Thousands (1,000s)
4. Tens of thousands (10,000s)
5. Hundreds of thousands (100,000s)
6. Millions (1,000,000s)
7. Don't know

To calculate an average number the following figures were used:

- Tens set as 50
- Hundred as 500
- Thousands as 5,000
- Tens of thousands 50,000
- Hundreds of thousands 500,000
- Millions as 2,000,000 (this figure may be on the low side)
- Don’t know, just 2/300 responses – ignored

Calculation of weight averages for top 3 top three concerns

For the data used in Figures 7 and 8 the original question was put to respondents as follows:

What are the top three concerns for your business with regard to its online services underperforming in some way? Please rank your top three concerns with the option you are most concerned about ranked first:

- Loss of revenues
- Poor user experience
- Erosion of customer loyalty
- Inability to attract new customers
- Loss of competitive advantage
- Negative impact on company reputation
- Vulnerability to security threats
- Other (please specify)

The issue ranked first was given a score of 3, second a score of 2 and third a score of 1. Non selected issues were scored 0. For each issue the average score was then calculated. If all had ranked the same issue as most important is would have scored 3 on average, if none had selected a given issue it would have scored 0.

Appendix 2 - demographics

Figure 24: Countries (actual sample numbers)

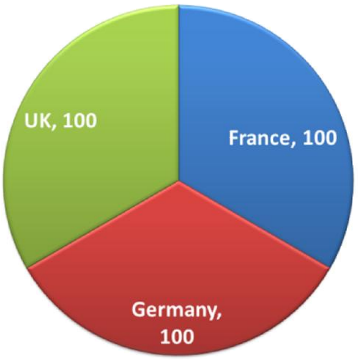


Figure 25: Number of employees (actual sample numbers)

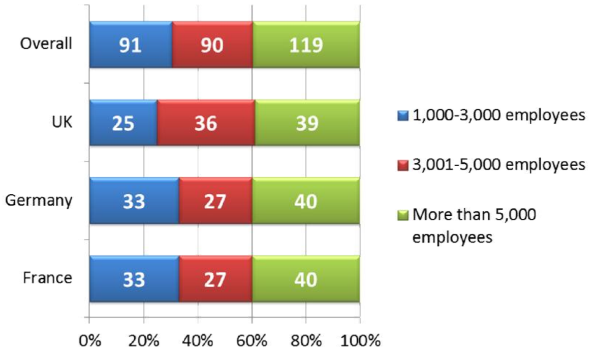


Figure 26: Industry sectors

Please note the small size of some samples, in particular pharmaceuticals which is added to "others" in the further analysis

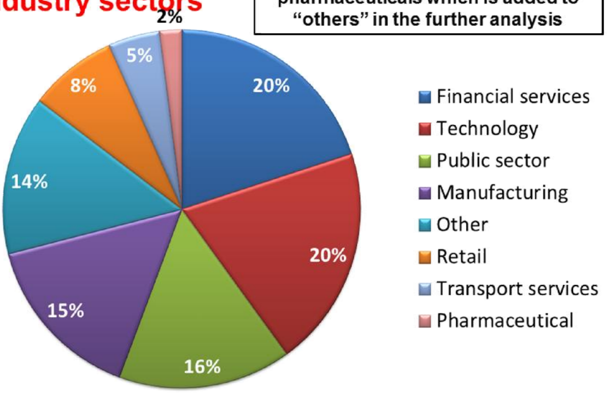


Figure 27: Industry sectors, by country (actual sample numbers)

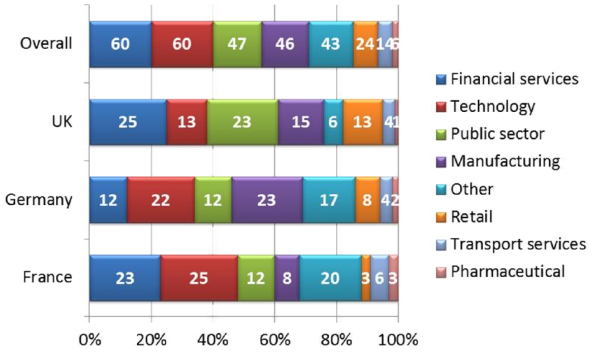
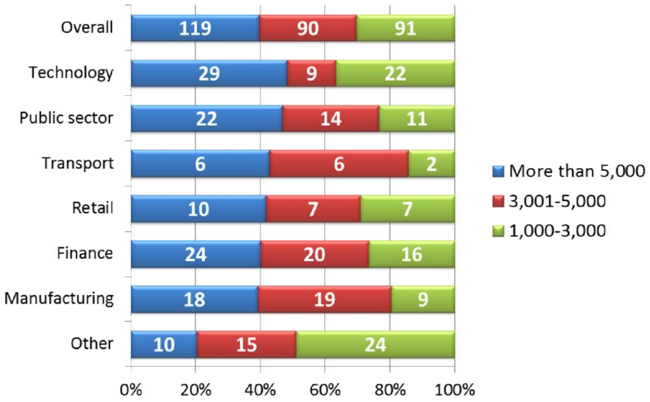


Figure 28: Industry sectors, by number of employees (actual sample numbers)



About Neustar

About Neustar

Neustar, Inc. is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, entertainment, advertising, and marketing industries. Neustar applies its advanced, secure technologies in routing, addressing, and authentication to its customers' data to help them identify new revenue opportunities, network efficiencies, cyber security, and fraud preventions measures. More information is available at http://www.neustar.biz.

Neustar SiteProtect: Keeping Businesses Safe from DDoS

To combat the dangers of DDoS, Neustar offers SiteProtect, a cloud-based, on-demand DDoS mitigation service. Activated through DNS or BGP redirection, SiteProtect scrubs away malicious traffic in the cloud, letting valid traffic flow to your infrastructure. To do this, SiteProtect relies on a large global mitigation network, featuring 15 IP anycasted scrubbing centres. Using diverse equipment from leading mitigation vendors, SiteProtect is designed to stop numerous types of attacks, including those involving the application layer, IPv6, and encrypted traffic. Technology diversity sets it apart from other mitigation solutions. By drawing on each vendor's strengths, SiteProtect can stop the multi-faceted assaults that are evolving rapidly and redefining the DDoS landscape. Backed by Neustar's 24/7 Security Operations Center – fully manned on-site by highly experienced experts – SiteProtect supplies the assurance businesses need. While it's best to prepare in advance, Neustar can emergency-provision SiteProtect should your business suddenly come under a DDoS attack. Learn more at
http://www.neustar.biz/services/ddos-protection

About Quocirca

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to get the most out of their online domains.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

Disclaimer:
This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.

All brand and product names are recognised and acknowledged as trademarks or service marks of their respective holders.

quocirca