

Digital Transformation Requires a "Subscriber-First" Approach

Leveraging DNS to Enhance the Digital Lifestyle

Publication Date: 13 January 2017

Kris Szaniawski



Executive Summary

Catalyst

Communications service providers (CSPs) are under intense competitive pressure to increase revenues and strengthen subscriber loyalty in markets around the globe. In order to thrive in this environment where over-the-top (OTT) players and other providers have utilized CSP networks to deliver innovative services, CSPs are now primed and ready to undergo digital transformation and develop new digital products and services that enhance the digital lifestyle of their subscribers.

Extensible DNS-based platforms and subscriber-centric applications are key enablers of digital transformation. They offer a more complete view of the customer and provide greater service agility to put subscribers in control of their own digital experiences.

Once considered to simply be the "phone book" of the internet, the domain name system (DNS) has moved beyond the realm of passive internet look-up functionality and is now at the heart of digital transformation.

DNS data can also be used to improve the customer internet experience, support personalization, improve customer interaction, and deliver new value-added services.

This report, conducted by Ovum's team of researchers and based on a global survey of 100 service providers, examines the benefits CSPs can gain from leveraging DNS to power their digital transformation efforts. It explores the changing business needs of CSPs, and how DNS contributes to a "subscriber-first" approach by optimizing the subscriber's internet experience and delivering personalized and differentiated services.

Key messages

- Reducing time to market for new services is a primary focus for CSPs, as is the need to establish a subscriber-first approach to improve customer engagement and strengthen brand loyalty.
- Security- and identity-based services are a clear CSP investment priority; research suggests that over 40% of CSPs have allocated budget to launch new security- and identity-based services in 2017.
- Understanding customer activity across all devices is a key component of digital transformation. It is important that CSPs discover new ways to manage customer activity, beyond relying on legacy data sources.
- DNS is an asset that all operators have access to, and it offers many benefits that can protect subscribers and children online, and provide proactive cyber defense against malicious attacks. DNS data can also be used to improve a subscriber's online experience, support personalization, improve customer interaction, and deliver new value-added services.

Recommendations for CSPs

- CSPs require extensible platforms and applications to gain a holistic view of the customer, enable real-time, personalized control and deliver value-added services that enhance the digital lifestyle. DNS leads the list of enabling technologies, which also includes established deep packet inspection (DPI), business intelligence (BI), and CRM data analytics.
- Too many in the industry are still unaware of the potential of DNS to personalize the customer experience and support a more subscriber-focused approach.
- CSPs need to make better use of new platforms and applications to accelerate digital transformation, and in particular they need to leverage DNS data to deliver increased personalization and meaningful customer interactions as they offer new value-added services. Such capabilities can be rolled out relatively quickly and inexpensively by leveraging an extensible DNS-based infrastructure.
- CSPs are increasingly evaluating niche/vertical software vendors as digital transformation partners. This trend will continue due to the growing importance of security and the need to deliver a real-time, end-to-end (E2E) view of customer activities.

Business Impacts

Market and business challenges

CSPs are under intense pressure in markets that are becoming more competitive and more proactive in jumpstarting digital transformation initiatives. However, a successful digital service provider (DSP) operating model is a complex framework involving many elements (see Figure 1), not the least of which is the use of new platforms and applications to deliver more agile, flexible and personalized services in order to support the subscriber's digital lifestyle.

Figure 1: Moving to a digital service provider operating model

| Strategy | Technology | Processes | People |
|---|---|---|---|
| <ul style="list-style-type: none"> ▪ Customer-centric ▪ Addressing adjacent industries ▪ Recurring service revenues and partnerships | <ul style="list-style-type: none"> ▪ Extensible and flexible architecture ▪ Focus on data and analytics to support personalization and new service creation ▪ App-driven product and service development | <ul style="list-style-type: none"> ▪ Agile and nonlinear processes and decision-making ▪ From two-year to two-month or two-hour development processes ▪ Beta testing with live customers | <ul style="list-style-type: none"> ▪ Shift from network to business impact ▪ Supporting closed-loop processes ▪ Crowd-sourced collaboration and improvement ▪ Employees incentivized to improve customer engagement |

Source: Ovum

CSPs are well placed to adopt a more customer-centric approach, given the huge network, operations, service and customer data resources to which they have access. Operators have an opportunity to improve how they both integrate and make use of all of their data resources to support various business-driven challenges, which include the following:

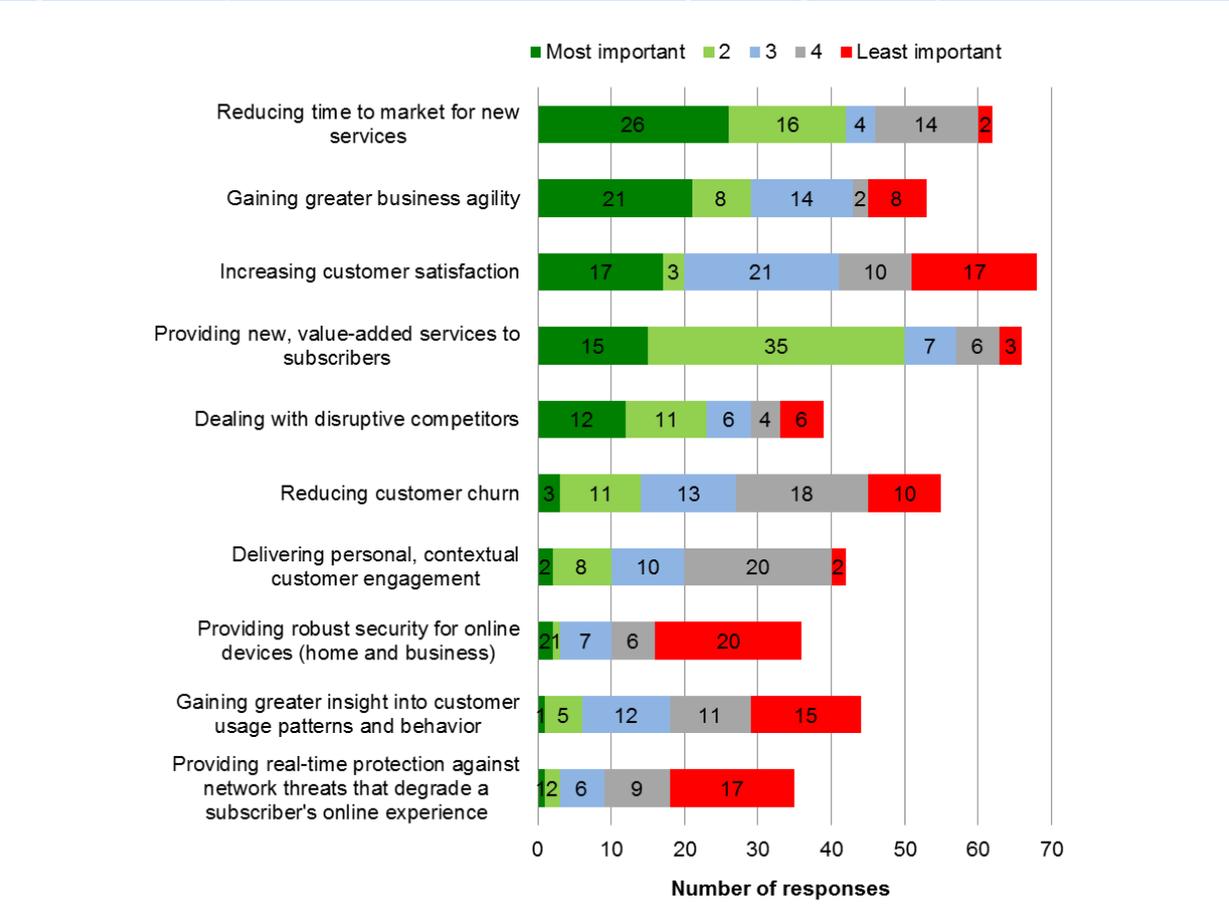
Reduce time to market: The long lead times for rolling out new services have a significant impact on both revenues and customer satisfaction levels. CSPs need automation, a policy-driven approach, and real-time information to accelerate business decision-making. Ovum's CSP survey shows that reducing time to market is the number one concern (see Figure 2).

Improve business agility: CSPs know they need to be highly responsive to client needs in order to compete with OTT players. To support greater service agility and flexibility, CSPs are looking to deploy predictive and contextually aware systems and analytics and a more flexible approach to reporting, data aggregation and real-time visibility of key operational metrics. These capabilities will enable delivery of the real-time personalized services that online customers increasingly demand.

Increase customer satisfaction: A subscriber-first approach is needed to improve customer engagement and loyalty. CSPs are looking to automate and enhance the customer internet experience at critical digital touchpoints.

Provide new value-added services: By offering personalized, subscriber-centric services, CSPs can realize greater top-line growth.

Figure 2: How important is it to deal with the following challenges within your business?



Source: Ovum

Technical challenges

The technical challenges facing CSPs are many, but some issues, such as strengthening security, improving wireless access and obtaining an E2E view of customer activity, are particularly acute.

Security is one of the biggest concerns for CSPs – in particular defending against malicious attacks such as ransomware, malware and distributed denial-of-service (DDoS). This is borne out by the Ovum survey which suggests that protecting the network from malicious attacks is now viewed by operators as the most critical technology challenge (see Figure 3).

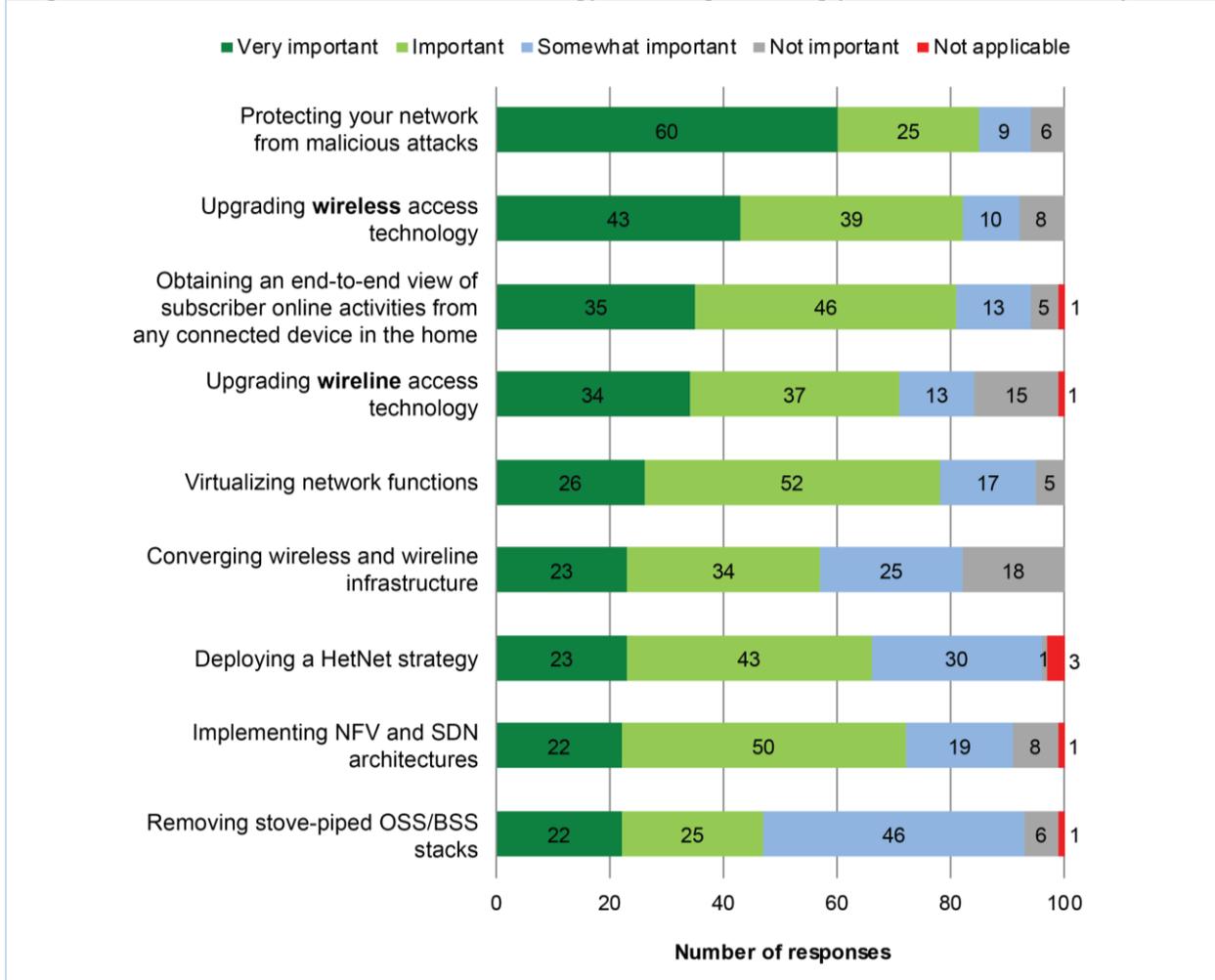
CSPs need to be able to deliver a growing list of capabilities that ensure subscriber safety, secure transactions, protect against botnets and provide identity/malware protection – ideally in a proactive manner. The increasing breadth and sophisticated nature of threats suggest the need for a "defense in depth" approach that makes use of multiple layers of security control. Ideally, this approach will combine more traditional methods with security and compliance solutions and intelligence-gathering tools, including big data security intelligence and analytics initiatives, and DNS-centric security approaches.

Security is one of the biggest concerns for CSPs – in particular defending against malicious attacks such as ransomware, malware and distributed denial-of-service (DDoS).

The need to obtain an E2E view of customer activity is deemed nearly as important. This concern is highlighted by the survey results, in which operators prioritize, over other network challenges, the need to obtain an E2E view of subscriber online activity across different devices. This is no surprise as operators need an E2E view of customer activity to deliver/enable integrated services, premium bundles and value-added services, as well as better targeted upgrades, promotions, notifications and usage alerts. Furthermore, these insights need to be delivered close to real-time to drive greater subscriber value.

However, it is important to note that all of the technology concerns listed in the Ovum survey are viewed as significant. None of them score low, which is an indication of the extent and seriousness of the issues facing CSPs and the need to adopt an integrated approach to address them.

Figure 3: What are the most critical technology challenges facing your business currently?



Source: Ovum

Investment priorities

To drive more business growth, rolling out and supporting new value-added services (e.g. parental controls) is currently the most urgent investment aim for CSPs, as confirmed by the Ovum survey. This is closely followed by the need to monetize the customer, including understanding and

Rolling out and supporting new value-added services (e.g. parental controls) is currently the most urgent investment aim for CSPs, as confirmed by the Ovum survey. This is closely followed by the need to monetize the customer, including understanding and anticipating customer needs and enabling relevant and compelling communications and upsell opportunities.

anticipating customer needs, and enabling relevant and compelling communications and upsell opportunities.

Security concerns are also viewed as important to CSPs, but the metric scores slightly less than the need to develop new services to support the digital lifestyle of its subscribers. This may seem

paradoxical since implementing a network security solution is considered crucial, but the incongruence here reflects the intense pressure CSPs are under to generate new revenues and demonstrate measurable growth.

As CSPs strive to increase metrics such as average profit per user (APPU) and average revenue per user (ARPU), they are looking to provide new services and a differentiated customer internet experience through improved customer interactions, more effective cross-sell and upsell, delivery of subscriber-defined content control and greater personalization.

New Subscriber-facing Services

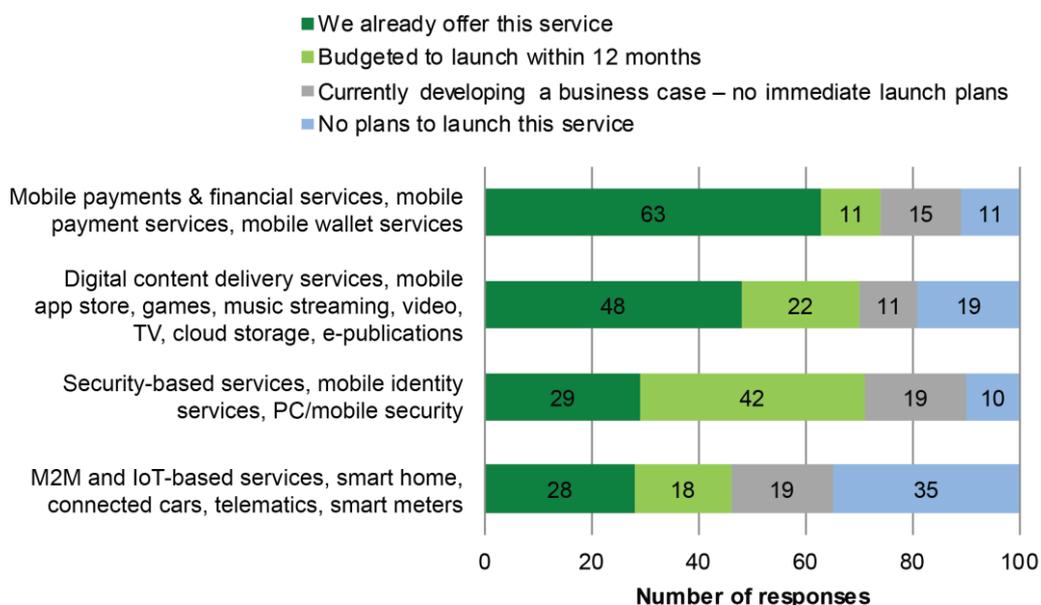
The opportunity for subscriber-facing services

This section looks at the relative importance of new digital services and where CSPs are directing their current investments. Fast delivery of these services is important in terms of a CSPs competitiveness and growth, but such service delivery also involves business and technical challenges.

Security- and identity-based services are a clear CSP investment priority; over 40% of CSP respondents have allocated budget to launch such services within the next 12 months (see the light green responses in Figure 4).

The scope of security services is extensive and includes both subscriber safety (e.g. protecting devices, shielding networks, protecting subscribers from phishing and malware, providing security breach notifications) and content compliance (e.g. blocking prohibited online content). Internet personalization (e.g. subscriber-defined content control at both household and device level, parental controls and monitoring, tailored alerts) is also closely linked.

Figure 4: Has your company allocated budget to any of the following services?



Source: Ovum

By contrast to security and identity-based services, mobile payments/financial services and digital content delivery services are more mature areas where services have already been launched, while machine-to-machine/internet of things (M2M/IoT) services are at an earlier stage in the investment cycle.

Benefits of new services: Personalized subscriber-facing services have the potential to increase subscriber spend, and, perhaps even more importantly, these services can attract new customers while retaining existing ones.

The personal nature of offerings such as advanced parental controls and internet personalization (e.g. setting screen time and content permissions for family members, monitoring and changing services features) helps CSPs enhance customer loyalty. The use of "live" internet triggers to activate customer messages is another form of personalization that can be used to boost customer satisfaction and reduce churn.

Given that customer acquisition costs exceed retention costs **four to one**, improving customer retention and the lifetime value of a customer is critical.

The challenges of delivering new subscriber-facing services

While demand for digital services is strong, there are digital transformation challenges facing CSPs in order to deliver them.

The lack of an E2E view of business processes and a shortage of internal technical expertise are the two biggest concerns for CSPs. A large proportion of surveyed operators described these as "extremely difficult" challenges. To adopt a more customer-centric strategy and support the types of services described earlier in this section, CSPs are looking to gain a real-time E2E view of customer activity.

Obtaining actionable insights across multiple devices is seen as something that is important to aim for but difficult to achieve. As M2M/IoT increases the number of connected devices, this need will grow.

Other issues operators face include the lack of clear internal champions, the difficulty of justifying the cost of creating new services and many business/operational process issues. Clearly CSPs feel burdened by the wide range of issues they need to overcome.

Lastly, most CSPs are still relying heavily on customer relationship management (CRM) data and billing/payment information as their predominant source of data when analyzing business problems such as customer churn or declining customer satisfaction levels. They are underusing potentially rich sources of interaction data such as website data, social media data and in-browser and online surveys. Additionally, the value that DNS data provides in delivering a single view of the customer is often misunderstood by CSPs.

Leveraging DNS to support subscriber-facing services

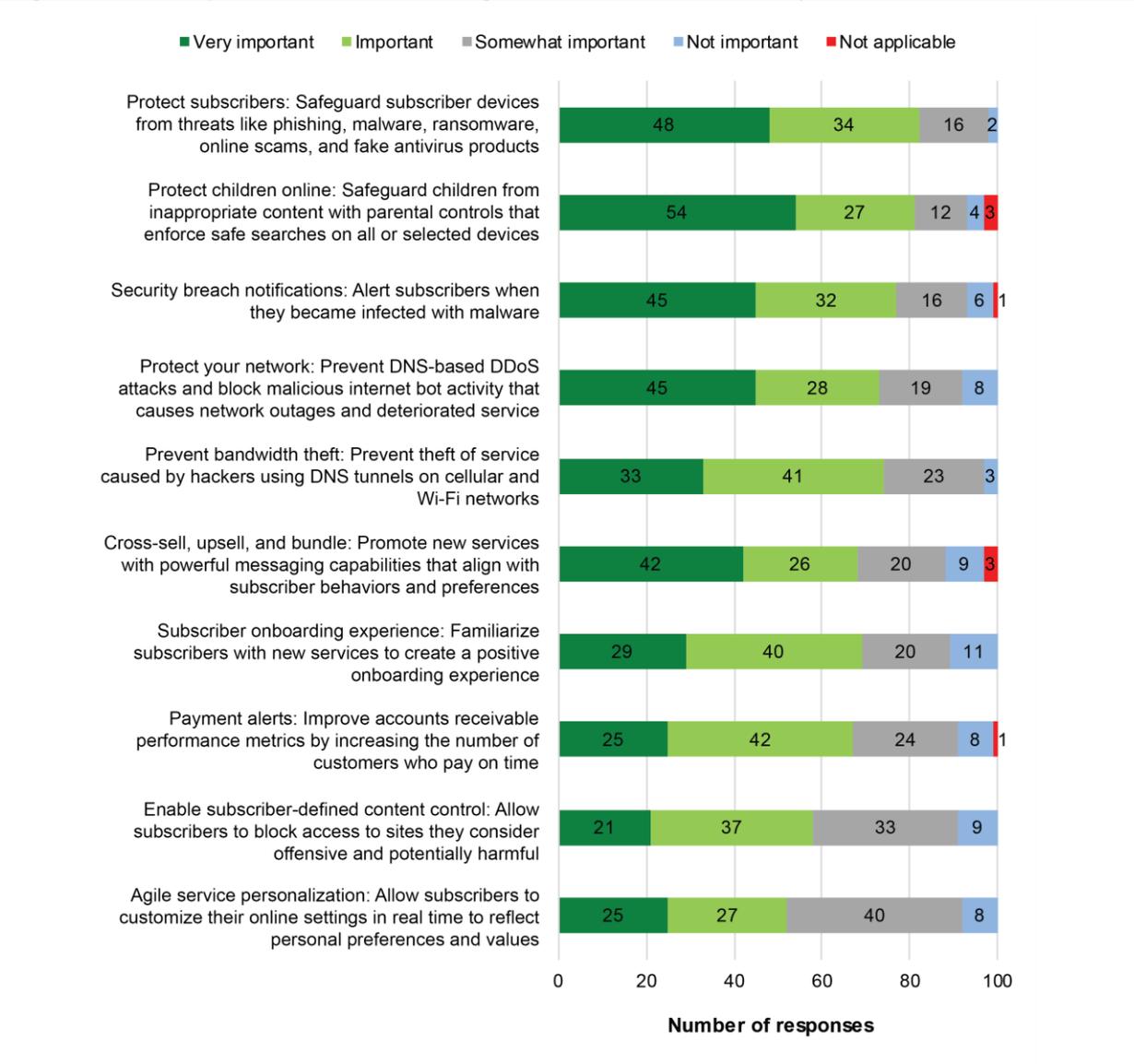
Almost a quarter of operators are unaware of the power of DNS in informing and potentially improving the customer experience, according to the global survey.

DNS is primarily viewed by CSPs as a means to protect subscribers and children online, defending against malicious attacks (e.g. malware, DDoS), preventing fraud or blocking inappropriate content (see Figure 5).

DNS data is clearly overlooked as CSPs struggle to get a single view of the customer.

The capacity for DNS to enhance growth is not rated particularly high. CSPs appear to understand that DNS-enabled services can adjust security controls in real time, but their perception is that this same capability cannot be used to support personalization, subscriber-defined content control, customer communication and cross-sell. And, as we saw earlier, there is an urgent need to roll out new value-added services to increase profit. There is a clear mismatch between perception and reality.

Figure 5: How important are the following DNS-enabled services to your business?



Source: Ovum

Vendor partners

CSPs often play it safe with their choice in a digital transformation partner, citing large software vendors and network equipment providers as the players they are most likely to consider in support of their digital transformation efforts. There is a tendency for CSPs to choose a big-name vendor, safe in the knowledge that the vendor will make things work for them or risk damaging its own brand.

However, niche/vertical software vendors are also increasingly making operator short lists, suggesting that there is increasing confidence in their capabilities despite their size. When asked what type of vendor they would most likely choose to support their digital transformation efforts, 92% of CSPs expressed a positive view of niche/vertical software vendors.

Although the big names will remain attractive, we expect niche/vertical software vendors to appear with greater regularity on CSP short lists, especially where they have the ability to address security issues (which are an increasingly high priority for CSPs) and also offer platforms that enable the personalization of a subscriber's online experience that supports a "subscriber-first" approach.

Appendix

Author

Kris Szaniawski, Practice Leader, Service Provider Operations & IT

kris.szaniawski@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product were correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo

