BT Connect

# DNSSEC Industry Survey Results

November 26, 2012

## While most respondents agree DNSSEC can provide benefits, less than half have deployed or plan to deploy within two years, largely due to perceived deployment complexity.

The inaugural BT Diamond IP DNSSEC survey garnered responses from 120 participants from a variety of organizations. DNS security extensions (DNSSEC) is Internet standards track technology having been codified within the Internet Engineering Task Force (IETF). The goal of DNSSEC is to enable resolvers making DNS queries to receive assurance that the corresponding query answers are authentic. DNSSEC utilizes asymmetric key cryptography technology to perform query validation. Each set of resource records is digitally signed by the zone publisher. The recipient of the query answer may validate the answer using the corresponding digital signature and public key[1].

A resolver may thus validate a DNS response and cache the answer as a secure response. Without DNSSEC, a DNS attacker could provide a falsified response to the resolver, possibly directing the querier to the attacker's website. The impact is broader than a single user as the resolver caches this information, which may be supplied to other queriers requesting the same information. The highly publicized DNS caching vulnerability discovered by Dan Kaminsky in 2008 made such cache poisoning attacks simpler to execute.

The only definitive solution to cache poisoning attacks is DNSSEC. DNS administrators can provide secure responses to DNSSEC-validating resolvers by signing their zone information.

## Key Findings

- Only 13 per cent of respondents have deployed DNSSEC signed zones in production and another five per cent are in the process of deployment. Even fewer have configured their caching recursive servers for DNSSEC validation with eight per cent having production deployments and another nine per cent progressing in deployment.
- Despite modest deployments, nearly two-thirds of respondents agree or strongly agree that DNSSEC can provide organizational benefits and that DNSSEC technology is mature enough to deploy reliably. On the other hand, over half of respondents agreed that DNSSEC provides limited value until more validating resolvers are deployed, highlighting the "chicken and the egg" challenge for DNSSEC deployment.
- Respondents generally agreed but were a bit unsure about supplementing DNSSEC deployments with hardware security modules (HSMs) with nearly half being neutral and over a third agreeing.
- Leading obstacles to DNSSEC deployment were complexity of deployment and the inability to demonstrate a strong business case. Training issues and complexity of ongoing DNSSEC management caused concern as well.
- Because DNSSEC requires knowledge of both DNS and cryptography to some degree, education and training programs may help improve industry awareness of the operation, benefits, and administrative requirements for deploying and maintaining DNSSEC secured resolution.

"DNSSEC helps allay concerns of website hijacking and related attacks that seek to corrupt DNS responses."

**Michael Dooley**
**IPAM expert**

[1] For more information about how DNSSEC works and is configured, please read our free DNSSEC white paper available at www.btdiamondip.com/dnssec.

“

Broad-based DNSSEC deployment requires organizations to both sign their zones, securing their name space, and to validate DNS queries using DNSSEC, securing their caching servers.”

**Tim Rooney, BT Diamond IP product management**

## Introduction

In October 2012, BT Diamond IP conducted a survey regarding opinions about DNS security extensions (DNSSEC) deployment and relative merits. The goal of this survey was to gather feedback from IP and DNS industry participants regarding the status of DNSSEC deployment, deployment strategies and obstacles to deployment.

This is our first DNSSEC survey and we plan to conduct this survey annually in order to identify deployment trends. This is the approach used with our IPv6 industry survey, which has helped illustrate the trends for IPv6 deployment over the last several years.

All survey responses were automatically tabulated into a survey tool. Any individual skipped questions were not included in tabulations. Each chart highlighting unique responses in this report includes the number of valid responses for that particular question (e.g. n=100 indicates 100 responses). Percentages shown in charts may not equal 100 per cent due to rounding.

## DNSSEC Overview

On the surface, DNS is very simple: a user device asks a question and a DNS server supplies an answer. DNSSEC enhances this process by digitally signing each answer so the questioner can be assured the answer is valid and not one supplied by a third party attacker impersonating the queried server.

Drilling down a layer, a typical DNS query starts with an end user device application, say a mobile phone web browser, issuing a query to locate an IP address for a given web address. The device sends the query to its local DNS server. This local DNS server then traverses the DNS domain tree to locate the DNS server that is responsible for the web address, which in turn supplies the answer to the query.

The querying local DNS server is referred to as the recursive or caching server, while the server responsible for the particular name being sought is the authoritative server.

Successful DNSSEC validation requires both the query originator, generally the recursive DNS server, and the query answerer, i.e., the authoritative DNS server, to be configured for DNSSEC operation. The recursive server must be configured with trust anchors, which are public keys, used to validate signed DNS responses. The authoritative server must be configured to sign its DNS information, i.e., its resource records.

Trust anchors enable the recursive server to validate the signatures provided with known trusted keys. The keys associated with each signature are validated up each layer of the domain tree to the DNS root. Ultimately, when the configured trust anchor matches the DNS root zone public key, the resolution is considered validated and secure.

The authoritative server needs to be configured with public keys that correspond to private keys used to sign the DNS resource records in each DNS zone. Its parent zone administrator must also “vouch” for the zone’s keys to link the chain of trust up the domain tree at each layer. The authoritative DNS administrator must also update signatures and keys periodically to reduce the risk of signature and key compromise.

This DNSSEC survey seeks to identify leading opinions of respondents with respect to DNSSEC technology, implementation strategies for recursive and authoritative servers, and associated obstacles to deployment.

## Concern for DNS security

We asked survey respondents about their level of concern for each of these two key areas, signing zones and validating DNSSEC responses. Results are summarized in Figure 1, which indicate slightly higher concern with the need to sign zones than with configuring caching servers for DNSSEC validation. This is likely due to the relatively higher level of initial and ongoing administration required with signing zones.

Summarizing both cases, about 30 per cent of respondents expressed a large concern with DNSSEC, expressing some urgency in the need to implement, while another 50 per cent indicated moderate concern, and 20 per cent low concern.

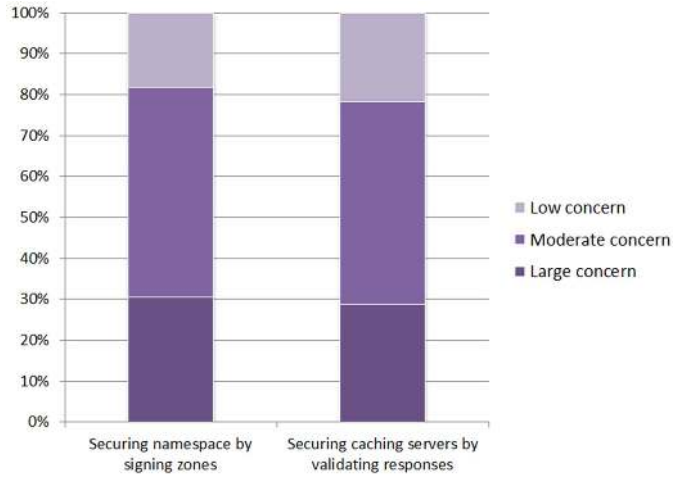


**Figure 1: Concern about DNS security (n=115)**

## DNSSEC Deployments

Survey respondents were asked about where they stood with deployment of DNSSEC, both for DNSSEC validation deployment on recursive servers and for DNSSEC zone signing on authoritative servers. About 10 per cent indicated they had already deployed zone signing and 11 per cent validation, while another 15 per cent and 10 per cent respectively are in the process of deploying DNSSEC. Eighteen per cent of respondents indicated they plan to sign their zones within two years, while 23 per cent responded they would configure DNSSEC validation within the same time horizon.

An even 18 per cent are currently assessing deployment though remain undecided for both signing and validating configurations. Over a third of respondents have not considered or assessed DNSSEC deployment at this stage.

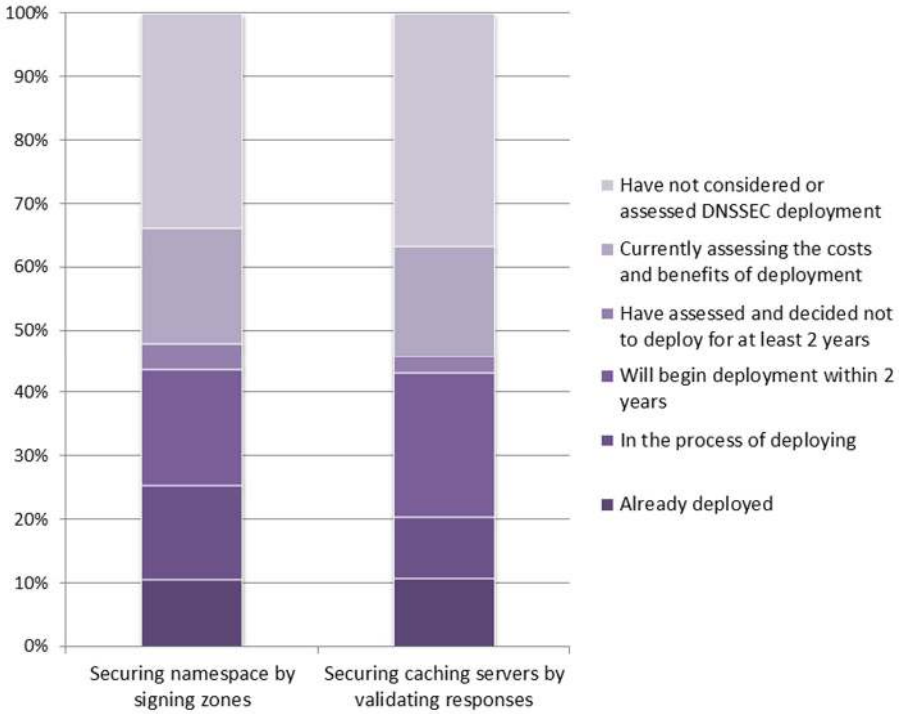


**Figure 2: DNSSEC Deployment Status (n=114)**

## DNSSEC Value

We asked survey respondents about the perceived value of DNSSEC itself, as well as particular configuration options, with results summarized in Figure 3. Despite the lackluster deployment volume brought out in Figure 2, discussed in the prior section, nearly two-thirds of respondents agreed or strongly agreed with the statement that DNSSEC can or does provide value to their organization. Nearly 60 per cent likewise agreed that DNSSEC technology is mature and can be reliably deployed within their networks. On the other hand, and perhaps explaining the modest deployments, over half agreed or strongly agreed that DNSSEC is of limited value until more DNSSEC validators are configured (52 per cent) and that deploying and maintaining DNSSEC is very complex (51 per cent).

If we assign a weighted average to respondents' answers to summarize the level of agreement by assigning the proportion strongly agreeing 5 points, agreeing 4 points, neutral 3, disagreeing 2 and strongly disagreeing 1 point, we derive a score of 3.73 out of 5 for the DNSSEC benefits statement and 3.67 for the maturity statement. Meanwhile the scores for DNSSEC complexity and the need for more validators was 3.57 and 3.50 respectively.

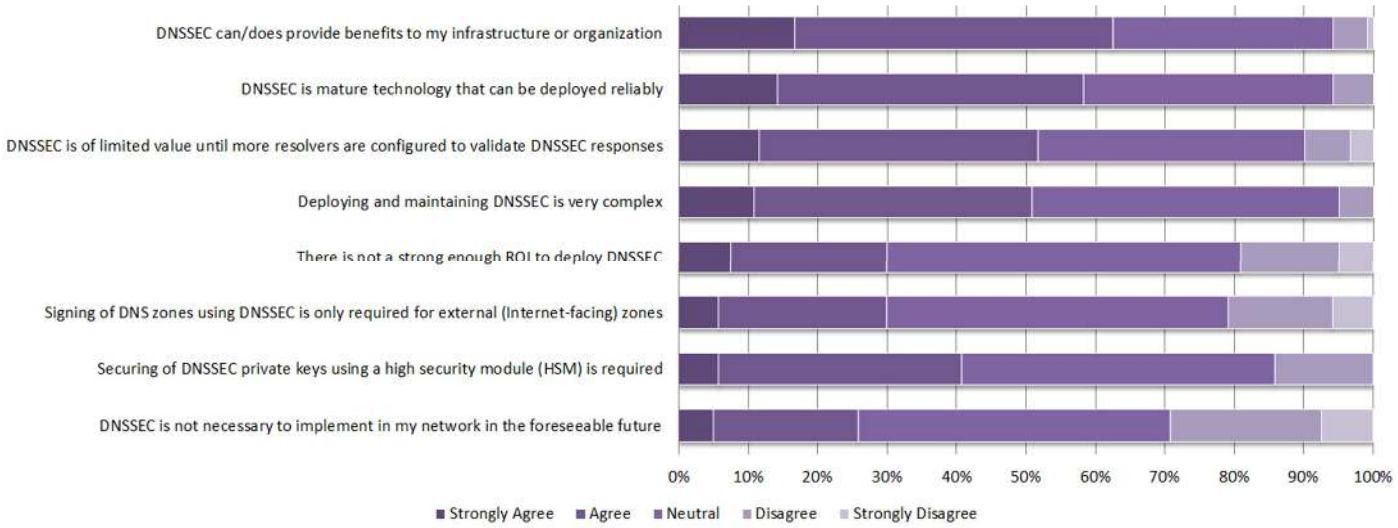


**Figure 3: Perceived Value of DNSSEC (n=120)**

Regarding the return on investment (ROI) for DNSSEC, respondents were split with 31 per cent feeling a strong ROI cannot be demonstrated, 19 per cent feeling ROI can be shown, and 51 per cent responding neutrally, for a weighted average score of 3.13. A similarly neutral proportion felt that DNSSEC zone signing is required for Internet-facing (external) zones only, yielding a 3.09 score.

We also asked respondents their thoughts on the use of hardware security modules (HSMs) to secure DNSSEC private keys. If an attacker should gain access to the private keys for a given zone, the attacker could effectively impersonate the zone by signing arbitrary zone information while effectively validating the data up the chain of trust due to use of the legitimate private key in the signing process. Clearly, one must consider securing private keys for each signed zone. An HSM can be deployed to securely store DNSSEC private keys. Using the crypto-API PKCS#11, the DNS server can send data to be signed to the HSM and the HSM, using the appropriate private key, can return the signature, without the private key ever leaving the HSM, keeping it secure. In terms of survey respondents' disposition on the need for an HSM for DNSSEC, just over 40 per cent agreed or strongly agreed with the necessity of an HSM, 45 per cent were neutral and 14 per cent disagreed; no one strongly disagreed.

Concerning the statement that DNSSEC is not necessary for the foreseeable future, 26 per cent agreed or strongly agreed with this statement, while 30 per cent disagreed or strongly disagreed.

## DNSSEC Deployment Obstacles

We asked survey respondents about their top obstacle to deploying DNSSEC. Figure 4 highlights that the complexity of deployment ranked highest at 29 per cent with the inability to demonstrate a strong business case and staff training tying for second with 18 per cent each. The complexity of ongoing DNSSEC management ranked fourth with 15 per cent of respondents, followed by 12 per cent indicating their top issue is too few DNSSEC validating resolvers out there to justify zone signing. Interestingly, the lowest ranked obstacle was the inability to justify deployment based on a DNS security assessment. Respondents recognize that cache poisoning is a real threat and the attack vector was made simpler through Dan Kaminsky's discovery.

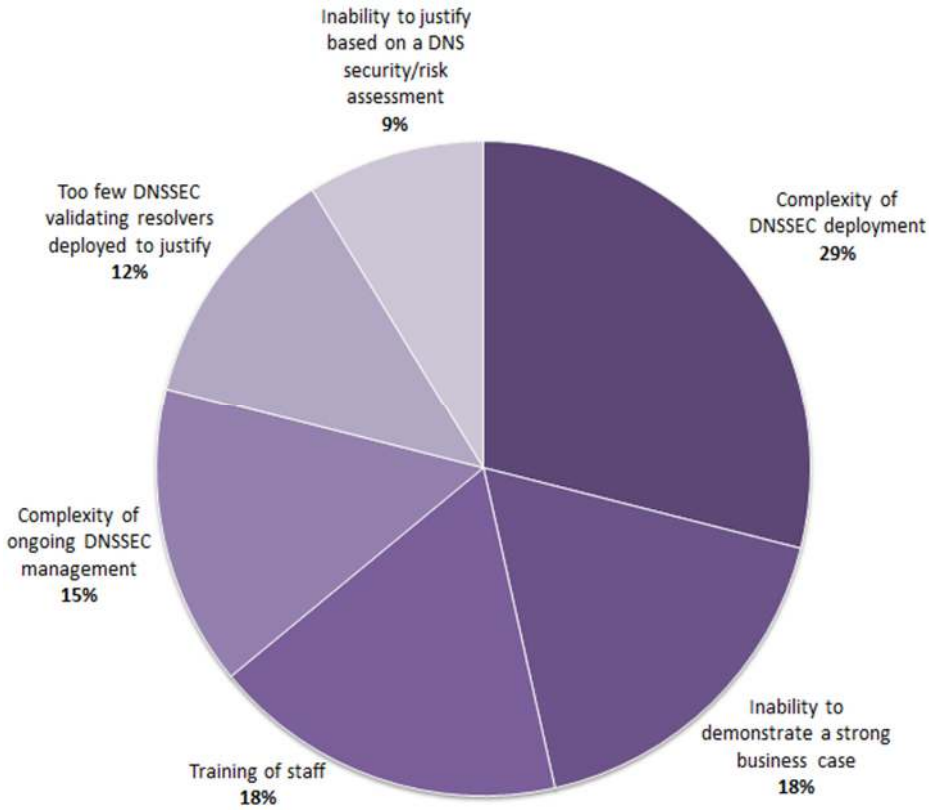


**Figure 4: Top obstacles to DNSSEC deployment (n=114)**

## DNS Security Implementations

To aid in automating DNSSEC operations, thereby addressing the concern regarding implementation complexity, several vendors offer DNS servers with DNSSEC automation features. The Internet Systems Consortium (ISC), publishers of BIND, the most widely deployed DNS platform, was the most popular answer with 36 per cent as shown in Figure 5. Microsoft, as of Windows Server 2008 R2 supports the current industry standard version of DNSSEC, came in second with 29 per cent. The remaining third of respondents was split among DNSSEC-Tools, OpenDNSSEC, Unbound and other products.

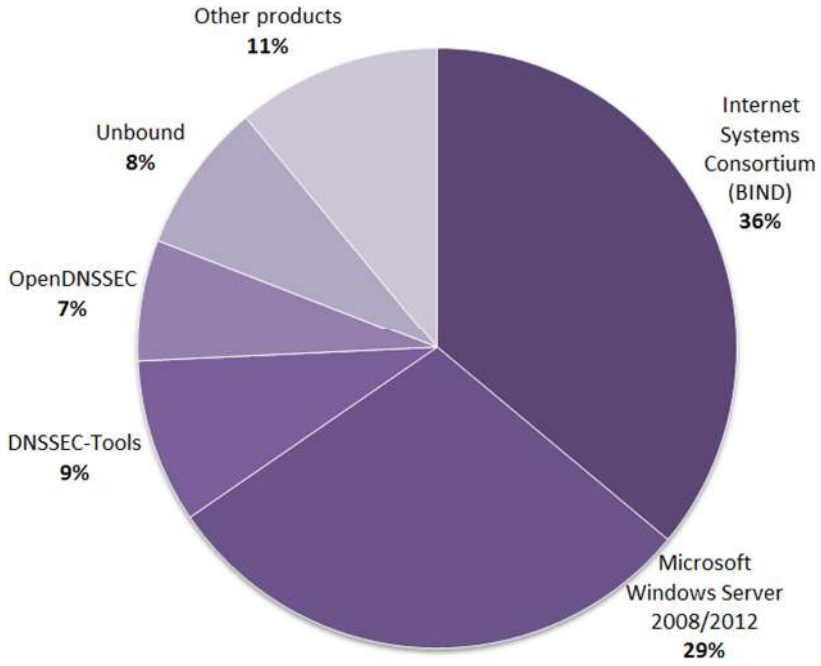


**Figure 5: DNSSEC vendor products in use or planned (n=136, multiple responses permitted)**

While DNSSEC technology secures the resolution process and effectively mitigates cache poisoning style attacks, it is not the end-all of DNS security. Several other forms of attack are possible against DNS severs including denial of service, reflector attacks, resolver redirection, server OS attacks and others. Hence, we asked the broader question of what security strategies respondents had in place or planned to implement. Results are shown in Figure 6.

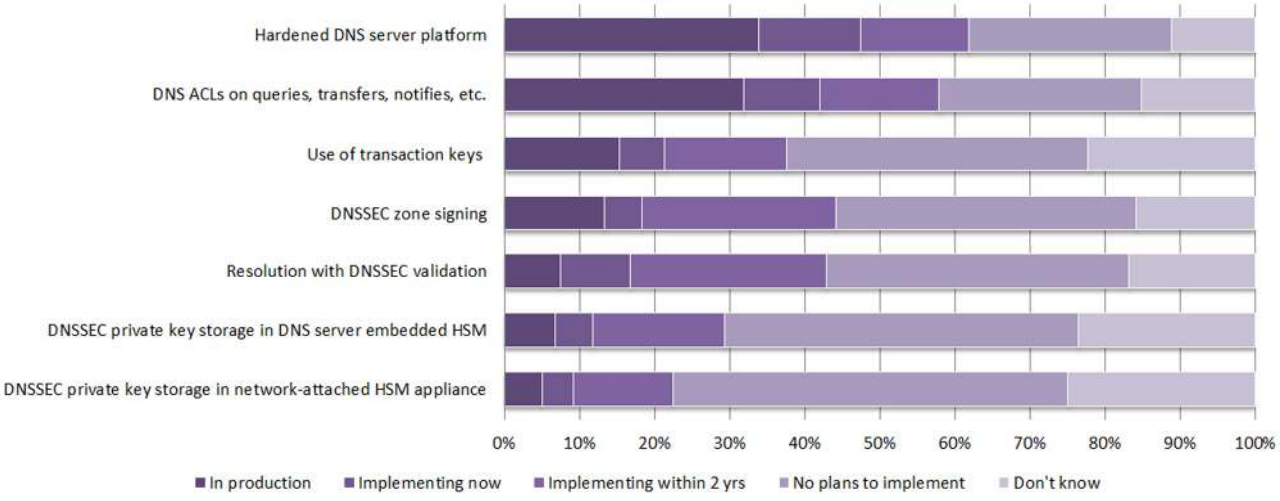


**Figure 6: DNS security strategies in use or planned (n=120)**

Over one-third of respondents to the question regarding general DNS security implementations have deployed DNS on hardened server platforms in production. Hardened platforms are not standard off-the-shelf systems but those with security-aware hardware and/or operating systems such as those found in most DNS appliance products. Typical steps in hardening include disallowing services, users, files or applications not needed for services running on the server, and running DNS in a jail. Nearly equally as popular, 32 per cent of respondents are configuring access control lists (ACLs) for DNS on queries, transfers and notifies on their production DNS servers. A lesser proportion, 15 per cent are using transaction signatures for updates and zone transfers in production.

Nevertheless, each of these three forms of DNS security ranks higher in terms of current and planned production than any of the DNSSEC-related responses, which followed. Thirteen percent responded that DNS zone signing is active in production while an additional 31 per cent are deploying or will deploy zone signing within two years. Eight percent have implemented DNSSEC validation with another 35 per cent planning to implement within two years.

Fewer respondents indicated deployment of HSMs to supplement their DNSSEC security, which can be implemented as either embedded HSM cards on the DNS server or as network-attached HSM appliances. The embedded approach generally appeared more popular, with seven percent having implemented HSMs as embedded production implementations, and five percent as appliances. Within the next two years, 23 per cent of respondents plan to implement an embedded HSM solution and 17 per cent plan on a network-attached HSM.

We asked survey participants who within their organizations is or would be responsible for DNSSEC implementation and management. We asked this for two reasons. First, DNSSEC implementation can be naturally separated into the"standard" DNS configuration process used prior to DNSSEC deployment, i.e., configuring resource records, and into a secondary signing process that digitally signs the resource record information. Second, DNSSEC technology centers on asymmetric key cryptography, a topic that sometimes glazes over the eyes of DNS administrators!

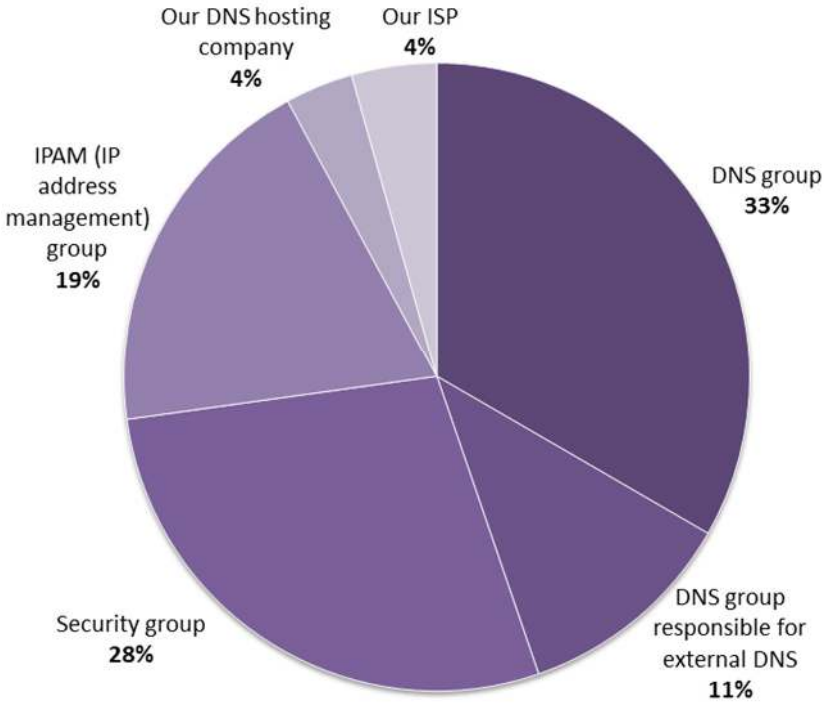


**Figure 7: DNSSEC responsibility (n=114)**

Responses indicate that 44 per cent leverage their DNS groups including 11 per cent explicitly responsible for external Internet-facing DNS, as responsible for DNSSEC implementation and management. But over one-fourth of respondents indicated that their security groups are responsible. Security groups can define the signature, key, algorithm, and rollover policies and apply it to the post-processing of DNS zone updates. Another 19 per cent manages DNSSEC within the IPAM team that manages IP address space as well as DNS together. Finally, four per cent each indicated reliance on DNS hosting providers or ISPs to implement DNSSEC on their behalf.

## Survey Demographics

Figure 8 illustrates the breakdown of survey respondents by organization type. Half of the respondents were from either educational or non-profit organizations, multinational enterprises or telecom/network service providers.

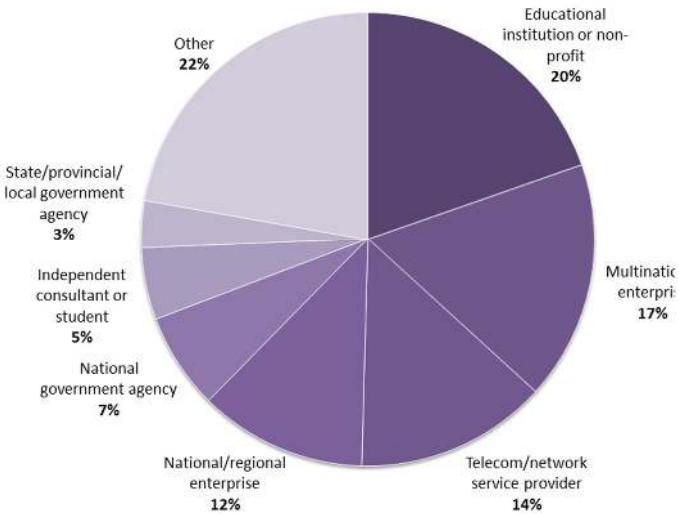


**Figure 8: Survey respondent organization types (n=106)**

The remaining respondents hailed from regional enterprises, governments or consultancies.

Figure 9 summarizes survey respondents' locations. Geographically, 62 per cent of respondents indicated they were from North America, 18 per cent from Europe, 16 per cent from Asia, thee per cent from Middle East/Africa and one per cent from Central/South America.

.

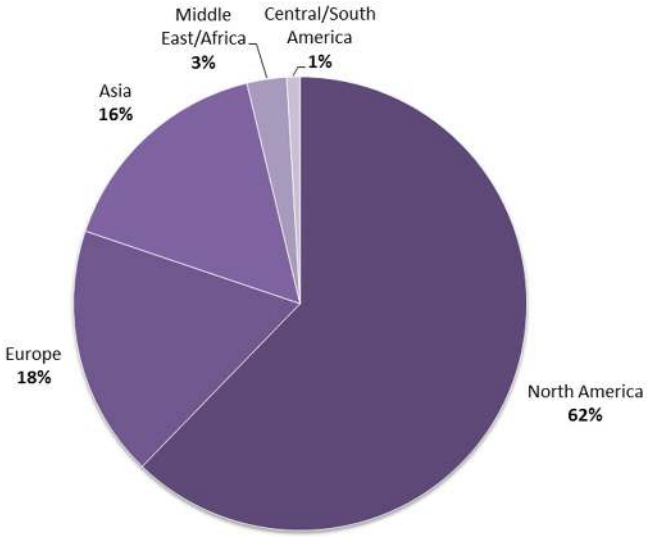


**Figure 9: Survey respondent locations (n=106)**

From a DNS zone sizing perspective, Figure 10 illustrates that 72 per cent of respondents each managed networks of less than 1,000 DNS zones, which is a relatively large number of zones for even a mid-sized organization. Sixteen per cent manage between 1,000 and 10,000 zones, and nine per cent between 10,000 and 100,000 zones. Three per cent of respondents managed DNS infrastructure of over 100,000 zones.

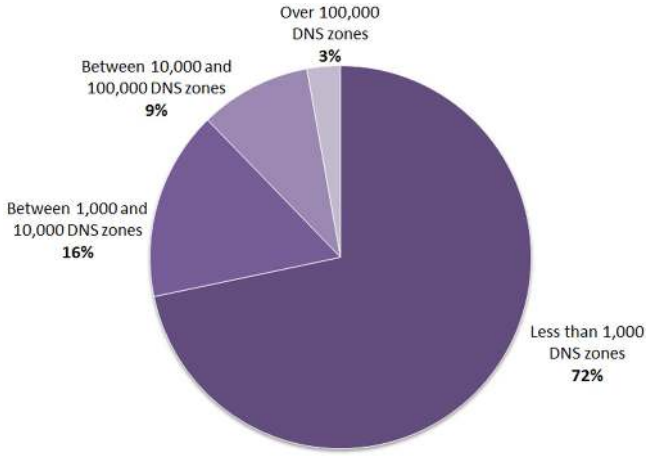


**Figure 10: Survey respondents' DNS zone sizes (n=106)**

## Conclusions

DNS provides the means for Internet users to reach your Internet servers. While most survey respondents see value and benefits with securing DNS resolution with DNSSEC, less than fifteen per cent have deployed DNSSEC due to complexity and an inability to demonstrate a strong ROI.

For more information about DNSSEC and about how BT can help you simplify your DNSSEC implementation, please visit www.btdiamondip.com.


Bringing it all together

## Offices worldwide


Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000