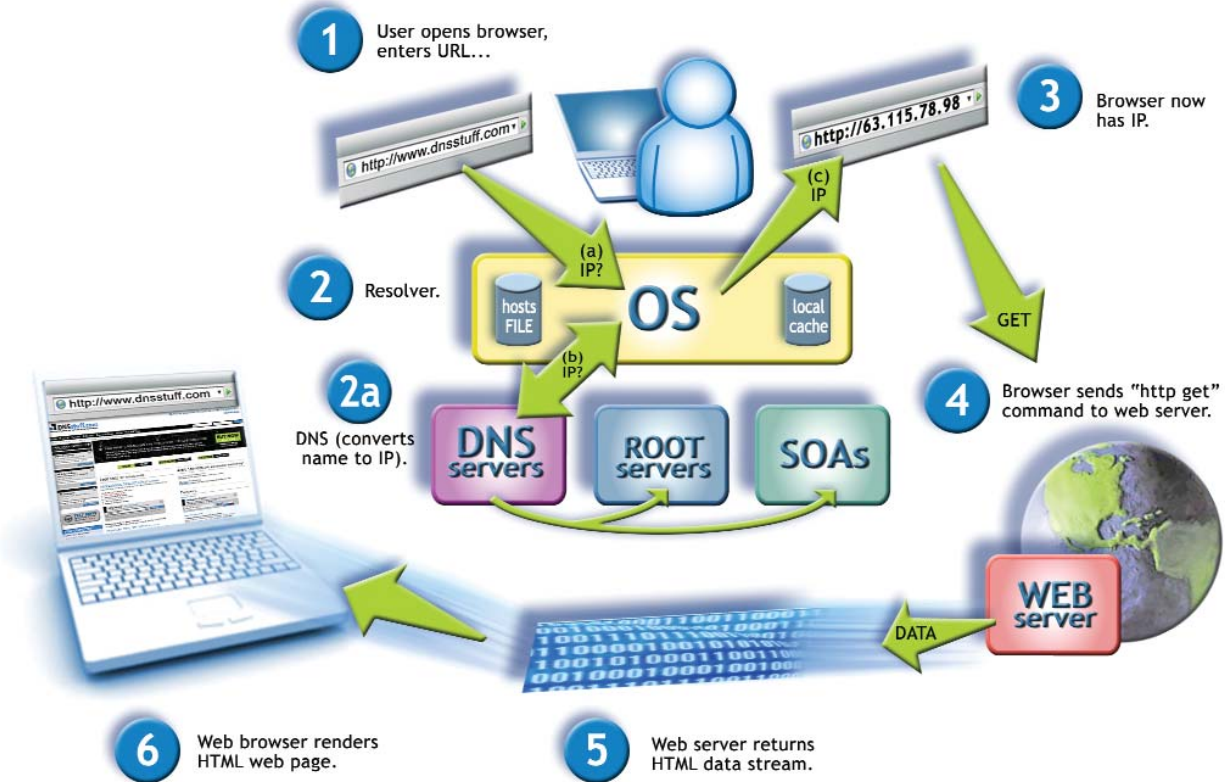


DNSstuff | How DNS Challenges Impact Business Continuity



Overview

In August and September 2008, DNSstuff invited its online enterprise customers to participate in a DNS survey, including specific questions about their DNS infrastructure. The survey was fielded through an invitation on DNSstuff.com. The goal of the survey was to better understand challenges associated with domain health, security and management. The following report represents top-line results of that survey.

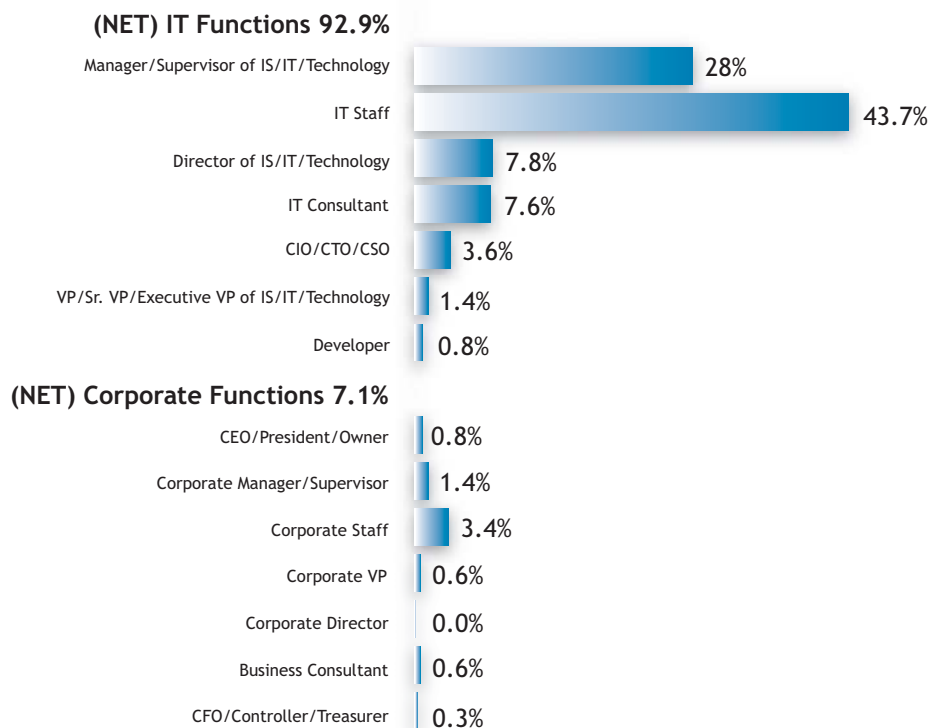
In addition, we have provided the results of internal research that identify trends in the response to the Kaminsky vulnerability.

Profile of respondents

Total respondents: 466

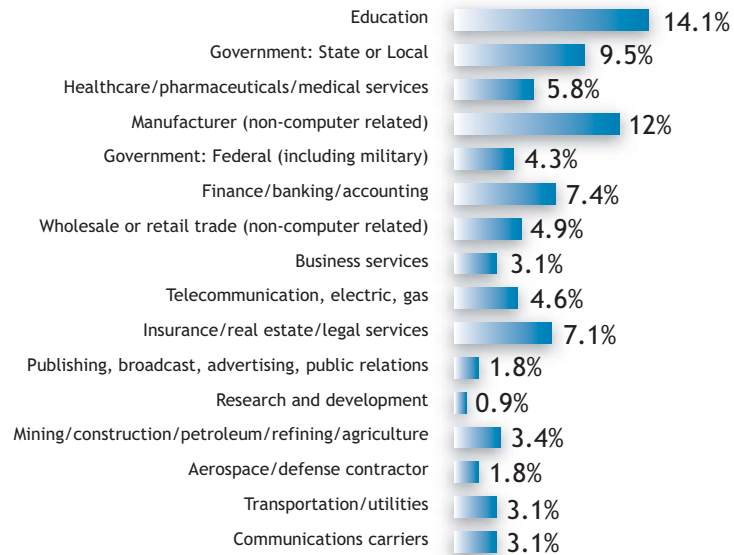
About 79 percent (367) of the respondents were qualified as being involved with the acquisition or management of DNS for their organizations. The chart below provides a breakdown of the percentage of overall respondents based on job function. This chart is followed by breakdowns of overall respondents, based on organization size and industry.

Which of the following best describes your primary job function?

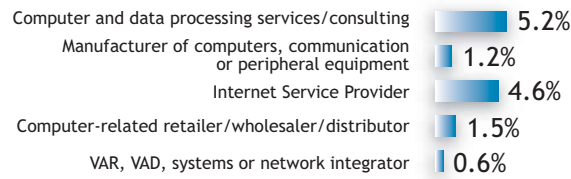


What is your organization's primary business or industry?

(NET) Non-Computer Related 75%



(NET) Computer related 13.1%

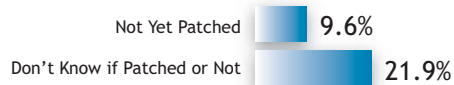


(NET) Other 11.9%

Time elapsed between CERT announcement and patching recursive DNS server

Our respondents indicated that 9.6 percent had not yet patched their DNS servers and 21.9 percent didn't know if they were patched or not. When asked why they had not patched their servers, 24 percent cited lack of knowledge about DNS; 45.5 percent answered that they didn't have the internal resources and 30 percent weren't aware of the vulnerability.

Patched DNS Servers?

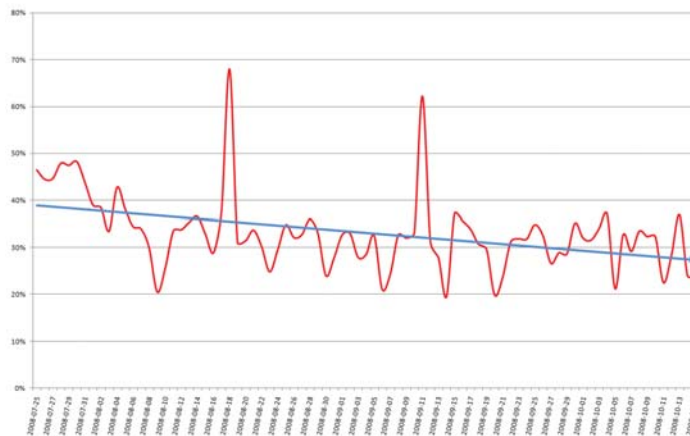


Why DNS Servers Were Not Patched



Vulnerability Checker Tool

Percentage of DNS Servers Tested as Vulnerable



Based on collaboration with Dan Kaminsky as the exploit was announced, we began to offer a tool to test for a users DNS server vulnerability. We have run almost eight million queries to date. The above graph indicates the percentage of servers deemed to fail this test.

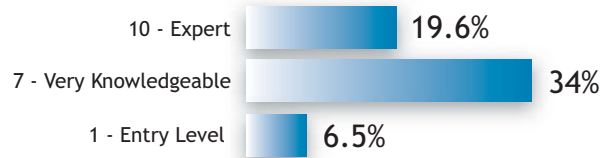
What makes a server vulnerable? The query source ports or the query IDs from a given server match or are easily predictable. Matching query source ports make it easier to spoof results to the DNS server, poisoning its cache. Matching query IDs are usually an indication of a misconfigured DNS server, while changing query IDs that are predictable also make DNS cache poisoning easier.

Level of DNS expertise within organization

QUESTION: *Please rate your level of DNS expertise within your organization (10 being expert level):*

19.6 percent of survey respondents rated their level of DNS knowledge as expert (10) while 6.5 percent rated their knowledge as entry level (1). The largest portion of respondents (34 percent) rated themselves as very knowledgeable (7).

Level of Expertise

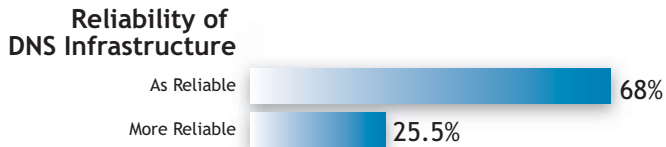


Reliability of DNS infrastructure versus other networking equipment

Almost 68 percent of survey respondents answered that their DNS infrastructure was as reliable as other networking equipment on their network. 25.5 percent indicated that their DNS infrastructure was more reliable. That means that 93.1 percent see their DNS infrastructure either as reliable as or more reliable than their other networking gear.

* NOTE: The ability to maintain quality data in DNS directly relates to the understanding that DNS data needs to be trustworthy and working for the world-at-large.

QUESTION: *How does the management and reliability of your organization's DNS infrastructure compare to other networking equipment on your network?*



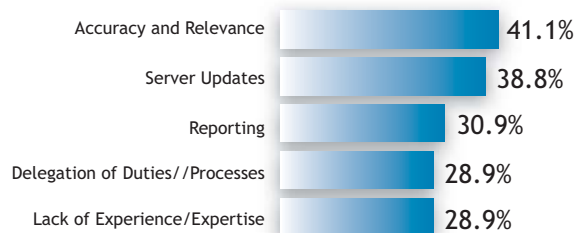
Challenges to DNS management

Accuracy and relevance (41.1 percent), server updates (38.8 percent) and reporting (30.9 percent) are the most significant challenges to DNS management. Delegation of duties and processes (28.9 percent) and lack of experience/expertise (28.9 percent) were still significant and yet tied in last place as challenges to DNS management.

A significant number reported all of these as important. So given that all of these things are important, respondents may not have a clear understanding of DNS related challenges. These are all important issues.

QUESTION: *What are your organization's most significant challenges when it comes to DNS management? (Check all that apply)*

DNS Management Challenges

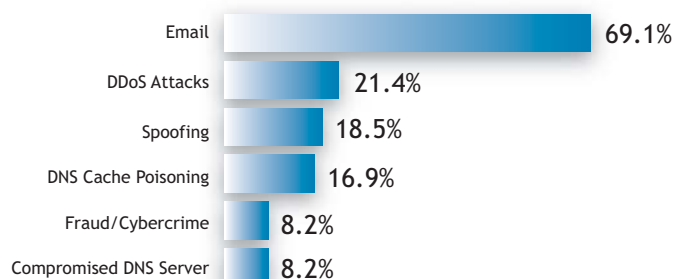


Most Common Issues Experienced with DNS

QUESTION: *What are the most common issues you have experienced with DNS?*

Email problems was reported to be the most common issue (by 69.1 percent) experienced with DNS, followed by DDoS attacks (21.4 percent), Spoofing (18.5 percent), DNS cache poisoning (16.9 percent), and fraud/cybercrime and compromised DNS server at 8.2 percent each.

Most Common DNS Issues



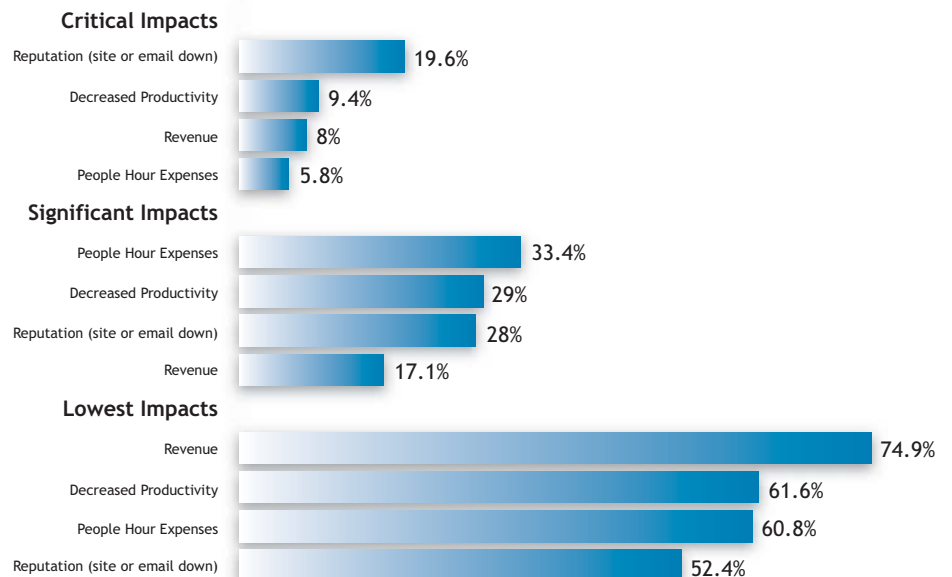
How DNS Challenges Impact Business Continuity

The survey listed four types of issues and three levels of impacts (based on severity). The results demonstrate some interesting patterns of response. This highest score for “critical” impacts were related to the reputation issue (having a site or email go down). Similarly the reputation issue had the highest combined scores for significant and critical impacts (47.6 percent).

Within the critical impacts category after reputation, came decreased productivity (9.4 percent), revenue (8 percent), and people hour expenses to solve (5.8 percent). Scores were higher across the board in the “significant” impacts category with people hour expenses to solve the highest (33.4 percent), followed by decreased productivity (29 percent), reputation (28 percent) and revenue (17.1 percent).

When it came to the lowest impacts, the issues came in with revenue the highest (74.9 percent), followed by decreased productivity (61.6 percent), people hours expenses (60.8 percent) and reputation impacts (52.4 percent).

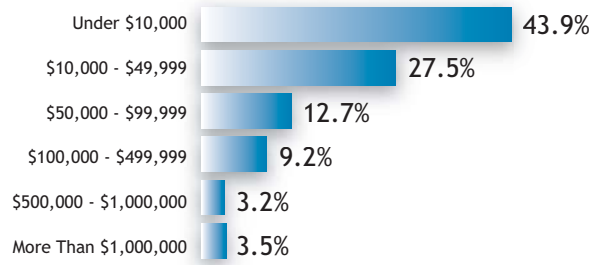
Clearly the highest level challenge associated with DNS relates to website and email availability with 47.6 percent of respondents ranking it significant or higher (critical).



Financial impact of one hour of lost email/internet access

Most respondents (43.9 percent) reported the financial impact of an hour of lost email/Internet access to be under \$10,000; 27.5 percent reported losses ranging between \$10,000 and \$49,999. The next largest category was \$50,000 - \$99,999 with 12.7 percent of respondents answering, followed by \$100,000 - \$499,000 (9.2 percent), more than \$1 million (3.5 percent) and \$500,000 - \$1,000,000 (3.2 percent). For almost 16 percent of respondents the financial impact of an hour lost was greater than \$100,000.

Financial Impact of 1 Hour Loss Email/Internet Access



Conclusion

The survey results suggest that there is a hunger for proper DNS management especially process, reporting, accuracy, patching and experience and best practices. Network managers see that email issues are by far the most relevant and secondly corporate reputation based on accessibility. It seems that IT staff are aware of the acute needs of availability and the way in which DNS interacts with deliverability. Business incur costs due to network inaccessibility (either email and/or web) that amounts to as much as \$11,800 per hour for businesses between 1 and 49 employees to \$1,865 for businesses having over 20,000 employees.

Additionally, almost 10 percent of respondents noted that they still had not patched their DNS servers for the cache poisoning exploit announced publicly in July. Bear in mind that this issue received unprecedented levels of coverage in the technology press and the business press. Overwhelmingly, this lack of patching was due to a “lack of internal IT resources.”

DNS - a rising attack vector

DNS is undoubtedly one of the most important technologies an organization will ever use. At the same time, most people don't work with it on a regular basis and just assume it will always be working. DNS issues can create enormous problems for businesses that rely heavily on the Internet.

The highly distributed nature of DNS can also further complicate problem solving as there are always unknown ramifications.

The DNS system is fundamentally based on trust. However, both malicious activities and human mistakes can significantly compromise the data the system holds. The question on every IT professional's mind is how to mitigate DNS risk as it relates to online business?