



ABBREVIATED REPORT

THE INTERNET AND DNS DEPENDENCY

Understanding the importance of uninterrupted Internet connectivity and the role of DNS among IT decision-makers at small, medium, and large organizations

Mazerov Research & Consulting, LLC

July 2007



CONTENTS

PURPOSE..... 1

HOW THE SURVEY WAS CONDUCTED..... 1

FINDINGS..... 2

Composition of the Audience 2

 Breadth of Company Types and Sizes 2

 Job Responsibility 3

 Size of IT Department 3

 Security Certifications Held by Respondent 4

IT Infrastructure 5

 Internet Dependence 5

 DNS Virtualization..... 6

DNS Security 7

 DNS Server Security 7

 Importance Factors in a DNS Solution 8

 Denial Of Service (DoS) Attacks..... 8

 DNS Compromises..... 9

 Most Catastrophic Area Affected in the Event of a Significant Internet Interruption 9

 Impact of a Major Internet Interruption..... 10

 Time Until an Interruption Becomes a Major Problem 10

 Awareness of DNS Solution Providers 10

SUMMARY AND CONCLUSIONS..... 11

 Lack of DNS Focus..... 11

 Seamless Internet Connectivity Isn't Simply a Business Commodity; It is the Lifeblood of Current Day Business Structure 11

 Many Companies Have Experienced Breaches of Their DNS Security 11

 Multiple Protection Methods to Protect DNS Uncover a Market Opportunity 11

THE INTERNET AND DNS DEPENDENCY

Understanding the importance of uninterrupted Internet connectivity and the role of DNS among IT decision-makers at small, medium, and large organizations

PURPOSE

The purpose of this research is to characterize and understand the IT marketplace for DNS servers and learn what will help solve the problems of IT professionals when they are protecting their infrastructure. This survey was conducted on behalf of [Secure64 Software Corporation](#) in order to better understand the needs of IT professionals and learn what problems they face in protecting their infrastructure. The survey was conducted independently and objectively by [Mazerov Research & Consulting](#); and at no time was Secure64 Software Corporation identified or even mentioned to any respondent as the sponsor of the survey.

HOW THE SURVEY WAS CONDUCTED

- Mazerov Research & Consulting, LLC of Denver conducted an Internet-based survey among 465 IT professionals in Feb/Mar of 2007.
- The participants in this national survey were decision-makers across a breadth of industries from government to manufacturing to media and tourism, and also included VARs and Integrators as well as ISPs. Virtually all economic sectors were included. The survey was also conducted across company size from under \$1 million to over \$250 million in revenue and from large and small IT staffs.
- A survey of 465 conducted in this method yields a margin of $\pm 4.5\%$.

FINDINGS

COMPOSITION OF THE AUDIENCE

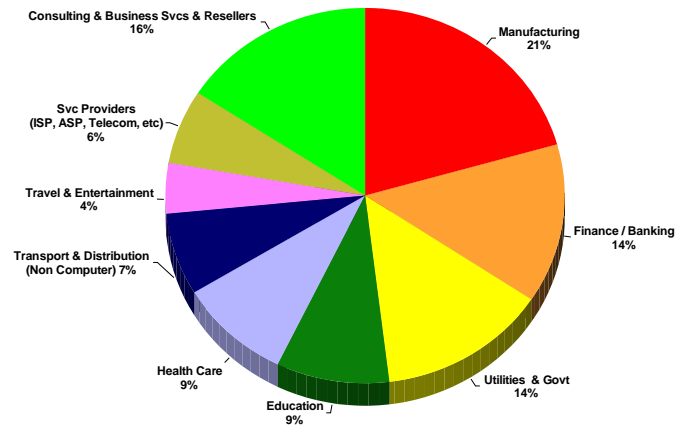
The survey was conducted among a breadth of company sizes and types, management levels, and size of IT department. All of the participants were decision-makers or significant contributors to their IT department's infrastructure and had oversight over DNS and related Internet connectivity issues. At no time was any participant in the survey informed as to the name of the sponsor or the exact reason for the survey.

Breadth of Company Types and Sizes

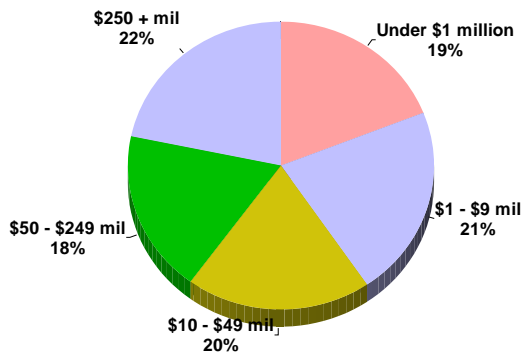
The survey participants were from a breadth of company and organization types from all over the United States. They were not balanced for an even distribution, but correct randomization generally produces a representative distribution. This graphic does not represent the distribution of all companies and organizations in U.S. business, but the company / organization types of the respondents who met the screening criteria.

In terms of annual revenue estimates, the respondents were also from a breadth of company sizes as well.

Company Type Groupings

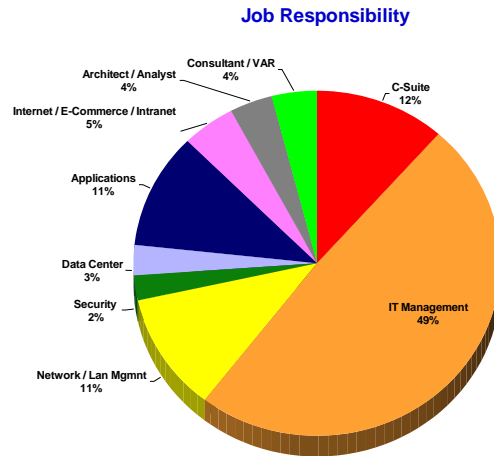


Company Size



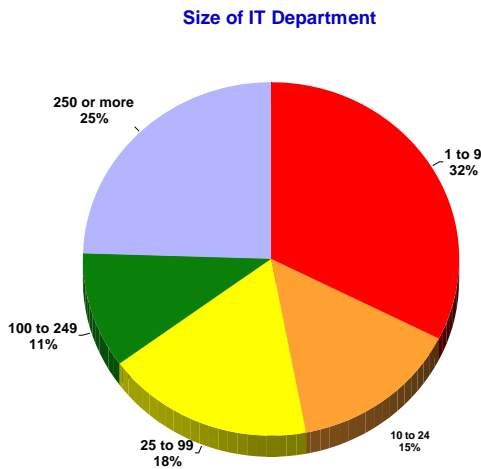
Job Responsibility

All of the participants were responsible for some area of their organization's IT functions, and the attached graphic shows that the greatest single group is in "IT Management" in general. The respondents' answers were carefully analyzed to learn if there were differences in the responses among different groups; and while there were some they did not impact the overall tone or learning from the research.



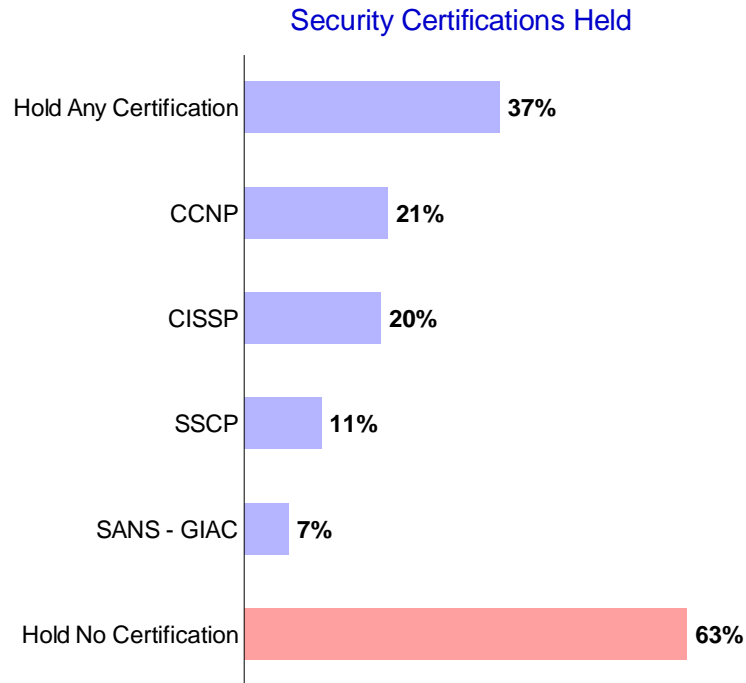
Size of IT Department

Reflecting the general breadth of the rest of the survey, the companies reflect a broad range of IT Department sizes.



Security Certifications Held by Respondent

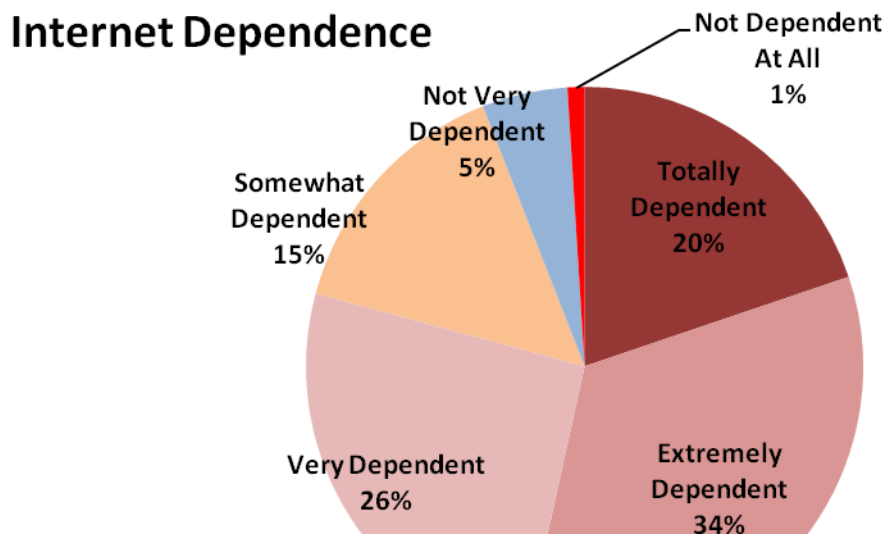
Overall, 37% of the participants held one or more security certifications (CCNP, CISSP, SSCP, SANS – GIAC). C-Suite and more senior IT Management professionals were significantly more likely to carry at least one security certification; and ironically the IT professionals LEAST likely to hold any security certification were those whose responsibilities were direct oversight of the company's Internet / Intranet or E-Commerce applications.



IT INFRASTRUCTURE

Internet Dependence

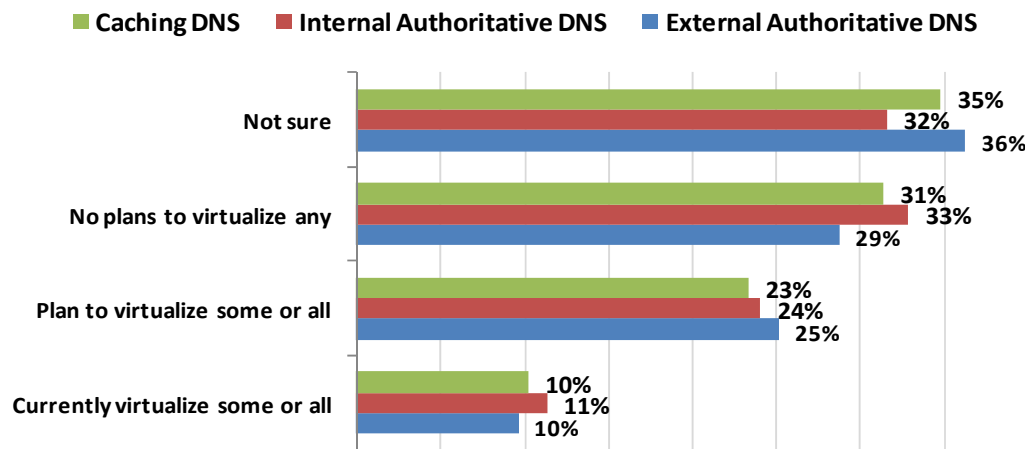
While organizations have varying degrees of Internet dependence based upon their business type and business processes, overall one-in-five companies (20%) is characterized by their IT management as “Totally Dependent” upon uninterrupted Internet connectivity and another 34% is “Extremely Dependent.” Overwhelmingly, the audience clearly indicates that their company or organization is highly Internet dependent, and only a small fraction says they are not.



DNS Virtualization

The particularly interesting learning here is the large number of IT professionals who said they were uncertain about their plans for DNS virtualization – approximately one-third of all the participants were uncertain about their future plans. About one-in-ten currently virtualizes some or all of their DNS, and the weighting is that slightly more respondents say they have no plans to virtualize than say they plan to virtualize some or all of their DNS.

What Are Your Plans for DNS Virtualization?

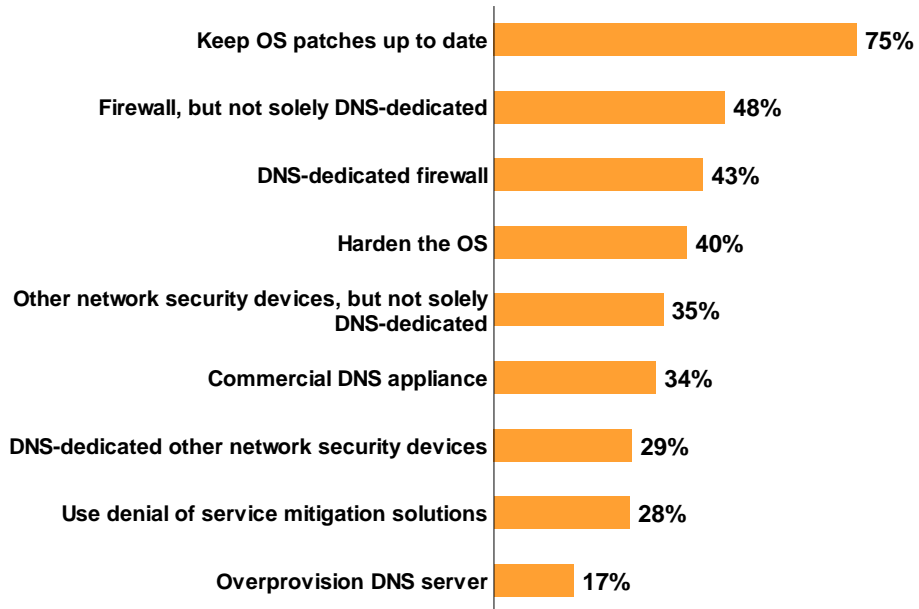


DNS SECURITY

DNS Server Security

Companies seek multiple, often overlapping, methods to protect their DNS. It is particularly interesting that on average companies use 3.5 methods to protect their DNS security, with the most prevalent being OS patch updates. Duplication of firewall protection is relatively common, with 10% of the respondents indicating they use BOTH a DNS-dedicated and a firewall not specifically dedicated to DNS protection; and 11% of the audience uses some other network security device for both DNS and non-DNS-specific protection.

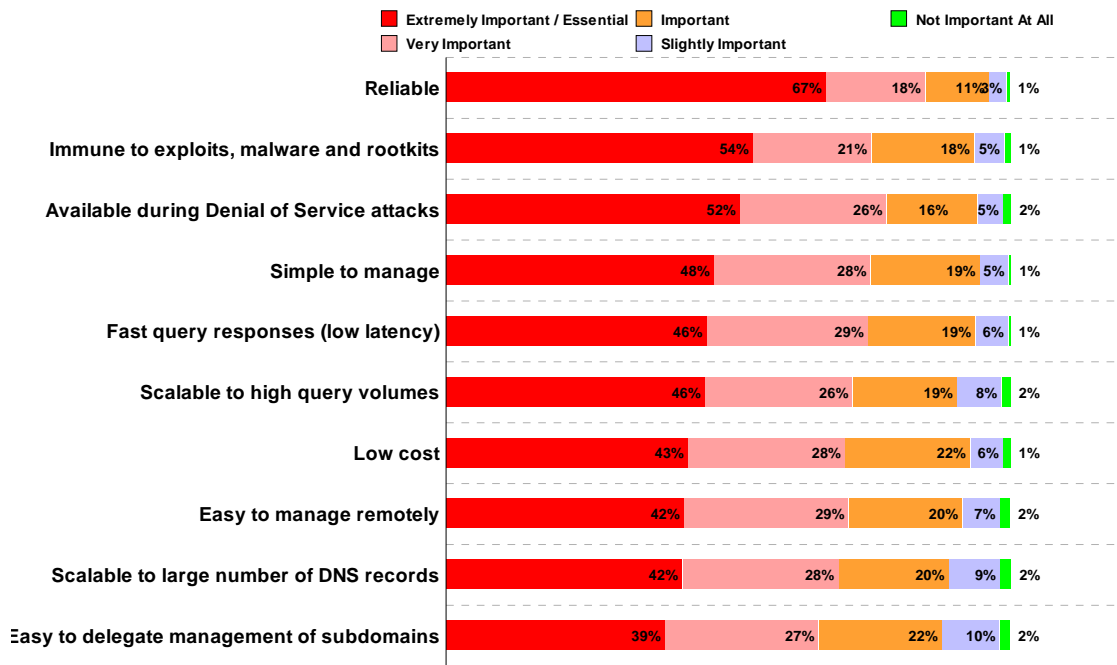
How do you ensure availability & security of DNS servers?



Importance Factors in a DNS Solution

Overwhelmingly, the most important factor in a DNS solution is that it works – it should be reliable, immune and available...but nothing is as important as reliability. While other specific factors drop off somewhat in the importance levels, it is also important to note that virtually nothing is unimportant when it comes to DNS. Cost appears lower on the list of important features – and we have seen this in other research we have conducted in this sector: a cheap solution is not trusted and falls down the list of important factors.

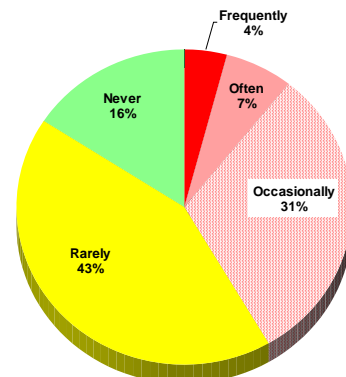
Importance in a DNS Solution



Denial Of Service (DoS) Attacks

DoS attacks are prevalent among the respondents, with only 16% having “never” experienced a DoS attack while over 10% of the IT professionals say they often or frequently receive DoS attacks to their network. What is also interesting is that, while a sum of 59% of the audience rarely or never experiences DoS attacks, a surprisingly high 41% of the audience experience DoS attacks.

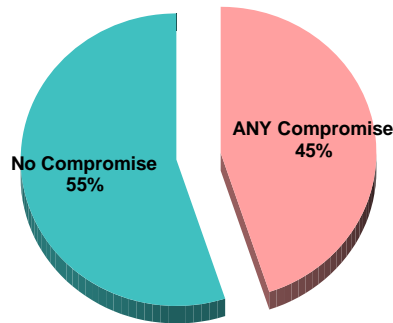
Frequency of DoS Attacks to Your Network



DNS Compromises

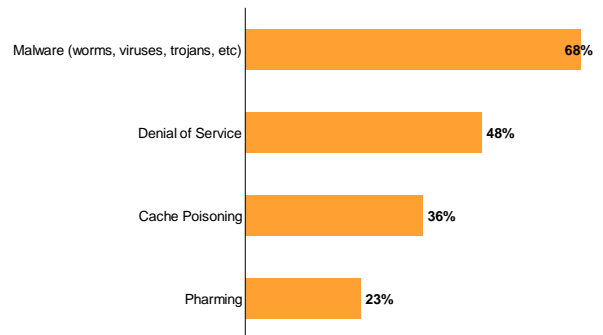
Nearly half (45%) of the participants had experienced a compromise of either their internal, external or caching DNS servers. By far the most prevalent problem has been with malware – with two-thirds of those who indicate they have been compromised noting that as the type.

Experienced Compromise of DNS?



Footnote: Any compromise of Internal, External or Caching DNS

Type of Compromise
Internal, External, Caching DNS



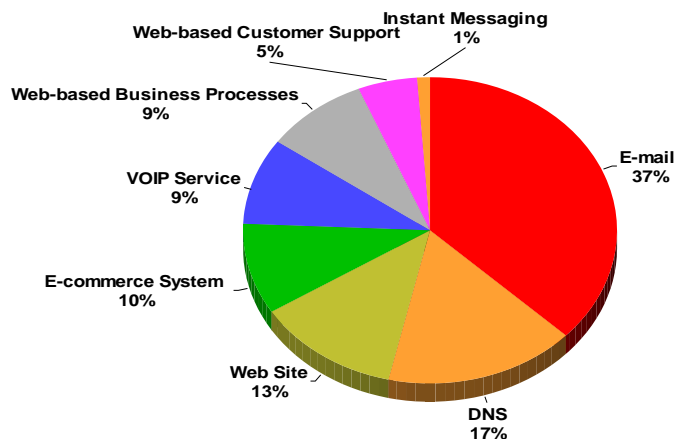
Footnote: Among those who had experienced some compromise of their DNS security.

Most Catastrophic Area Affected in the Event of a Significant Internet Interruption

Perhaps the most ironic aspect of this part of the survey is that DNS is a misunderstood part of the IT infrastructure. While 37% indicated that the loss of email and 13% indicated that the loss of access to the web would be the most catastrophic, the fact is that with the loss of DNS, all of these services would be largely unreachable. This indicates a clear misunderstanding of the role of DNS protection among the IT community, even among high-level IT management. DNS plays a significant role in the IT infrastructure, but it's relegated to the shadows.

These results may indicate that the most visible and potentially vocal complaints would come from the company's reliance on email and web connectivity – but DNS affects them all and is not thought of with the same criticality.

MOST Catastrophic Problem in Event of Significant Interruption



Impact of a Major Internet Interruption

The expected result of a significant interruption in Internet connectivity goes far beyond simple inconvenience or a slight loss in productivity. **A significant interruption of Internet connectivity has staggering expected impact:**

- Three-fourths of the respondents said their company would be likely to *lose productivity* and just over half (54%) said they would be unable to conduct basic business functions.

However, the implications of a significant Internet interruption go much further than short-term inconvenience:

- 40% say their company would “lose significant revenue”
- 39% say their “brand image would suffer”
- 30% would “lose customers”
- 12% feel their company would be likely to “go out of business”

Thus, seamless Internet connectivity is not simply a convenience, it is an absolute necessity. Therefore, protection of the IT / Internet infrastructure is critically important.

Time Until an Interruption Becomes a Major Problem

Professionals at different levels of the company have different thresholds for length of time until an Internet interruption becomes a significant problem. This and other research MR&C has conducted shows that minor interruptions of a few minutes overall are planned for and backup systems are in place to handle these inconveniences. But in this case the respondents were posed with a “significant interruption in Internet connectivity” that would have an impact on the company.

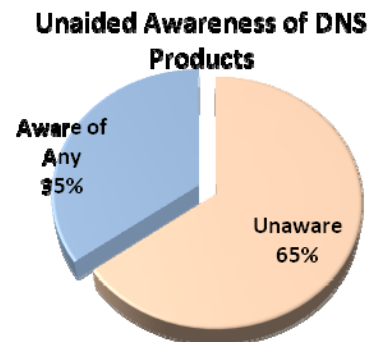
Overall, a significant interruption has lasting impact on the company at about 88 minutes. That is, in just under 1.5 hours the company begins to suffer long-term damage as a result of Internet connectivity interruption. Some areas are more sensitive than others such as customer support (79 minutes) and web-based business processes (86 minutes). It is important to reinforce that this is not merely a momentary lapse in connectivity, but a significant, catastrophic loss in Internet connectivity.

A significant interruption in Internet connectivity has a lasting impact on the company in 88 minutes or less.

The closer you are to the problem, the faster it causes pain. Front-line IT managers are significantly more sensitive to the timing issue, seeing a problem becoming significant in 72 minutes; while the C-Suite sees the problem becoming significant in 126 minutes. Likewise, the more dependent you see your company on Internet connectivity, the faster a problem becomes significant: 74 minutes for a company highly dependent on Internet connectivity; 100+ minutes for a company with lesser Internet dependence.

Awareness of DNS Solution Providers

No DNS solution provider has yet come to the forefront of the industry as a leader for the mindset of the IT professionals: *nearly two-thirds (65%) of the IT professionals were unable to recall even one provider of DNS solutions.*



SUMMARY AND CONCLUSIONS

While this is an abbreviated report for broad distribution, there are several overall conclusions that may be drawn with regard to the protection of the IT infrastructure.

Lack of DNS Focus

There is unquestionably a lack of understanding of the interplay of DNS security and how it relates to the connectivity of a company's IT infrastructure and Internet availability. Many IT professionals see the most visible and vocal areas such as email and web connectivity, and do not see the underlying issue that:

- Loss of email is a hindrance
- Loss of DNS is a calamity that affects all aspects of the IT and company infrastructure.
- Loss of connectivity has epidemic consequences

Seamless Internet Connectivity Isn't Simply a Business Commodity; It is the Lifeblood of Current Day Business Structure

The implications to a company or organization to Internet interruption are staggering beyond the simple inconvenience. IT professionals see potential for long-term, catastrophic harm done to their company – and this occurs in as little as 90 minutes. When one-in-eight say their company is likely to go out of business, 30% say they would lose customers, and 39% say their long-term brand image would suffer at their loss of Internet connectivity.

Many Companies Have Experienced Breaches of Their DNS Security

A surprising number of companies (41%) have experienced a compromise of their DNS, given the lack of publicity of such events. This seems to reinforce commonly held belief that most companies keep security breaches quiet.

Multiple Protection Methods to Protect DNS Uncover a Market Opportunity

Companies utilize multiple methods to protect their DNS, and while they may be duplicated and seem unnecessary, this is a typical method for IT infrastructure protection. However, the IT professionals also put a high value on ease of manageability, and with multiple methods of protection it makes the infrastructure more difficult and complicated to manage. Thus, a less complex solution may have market appeal. This does not mean that the solution has to be elementary - relying on simple interfaces for example. Rather, the more simple the overall solution is (e.g., fewer boxes and applications to manage), the more appealing a DNS product would be.

For more information contact:	Robert Mazerov President Mazerov Research & Consulting 303 741-2369 Hbobm@mazerovresearch.com Hwww.mazerovresearch.comH
-------------------------------	--