Arbor Special Report

Worldwide Infrastructure Security Report

2012 Volume VIII

ARBOR NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including the vast majority of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 250+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

Table of Contents

List of Figures

Overview

This report provides the results of Arbor Networks' eighth annual *Worldwide Infrastructure Security Report.* The survey covers a 12-month period from October 2011 through the end of September 2012. It was designed to collect the experiences, observations and concerns of the operational security community.

The information within this report provides a general resource for all network operators on key trends in security techniques, threats and other operational security issues.

The survey responses on which this report is based came from a broad range of organization types from all regions of the world. The majority of those completing the survey are directly involved in day-to-day operational security incident handling. This report is intended to provide a real-world view of the security threats that organizations face and the ways in which they mitigate those threats.

Survey Methodology

The 2012 survey was comprised of 193 free-form and multiple choice questions, a significant increase over the 132 questions in last year's survey. However, the survey was segmented into more sections with additional logic to manage question flow. As a result, the number of questions actually posed to each individual participant was reduced to only those that were relevant (based on earlier answers). This is in line with our goal to continually improve the quality of the survey data and the experience of those participating.

As in previous years, the survey addressed topics such as threats against infrastructure and customers, techniques employed to protect infrastructure, and mechanisms used to manage, detect and respond to security incidents.

Questions were split into sections on participants' security concerns, detected DDoS attacks and IPv6 strategies. Specific sections for data center service providers, mobile operators, MSSPs, enterprises, and VoIP and DNS operators were included. Additional sections regarding threats to the internal networks of both operators and enterprises were also added.

Many refinements have been made to clarify questions based on feedback from survey participants. From year to year, some questions have been added and some have been deleted in an effort to capture the most relevant information.

Key Findings

Advanced Persistent Threats (APTs) a Top Concern for Service Providers and Enterprises
Advanced threats are a well-established problem for enterprise network operators. This year's survey found an increased level of concern over 'botted' or compromised machines on provider networks. The increase in botted hosts is not surprising given the number and complexity of malware variants that exist, their rate of evolution and the consequent inability of Intrusion Detection Systems (IDS) and Anti-Virus (AV) systems to fully protect them. Looking ahead, there is even more concern about APT, industrial espionage, data exfiltration and malicious insiders.

DDoS: Attack Sizes Plateau; Complex Multi-Vector Attacks on the Rise
This year's results confirm that application layer and multi-vector attacks are continuing to evolve while volumetric attacks are starting to plateau in terms of size. Attackers have now turned to sophisticated, long-lived, multi-vector attacks—combinations of attack vectors designed to cut through the defenses an organization has in place—to achieve their goals. Multi-vector attacks are the most difficult to defend against and require layered defenses for successful mitigation.

Data Centers and Cloud Services are Increasingly Victimized

Nearly half of respondents experienced DDoS attacks targeted at their Internet data centers during the survey period. Ninety-four percent of these respondents report seeing DDoS attacks regularly. As more companies move their services to the cloud, they now have to be wary of the shared risks and the potential for collateral damage. With e-commerce and online gaming sites being the most common targets, according to survey results this year, sharing data centers with these organizations brings some risk.

Ideology Primary DDoS Driver

The top three most commonly perceived motivations for DDoS attacks are political/ideological, online gaming and vandalism/nihilism. These are largely acts done in reaction to real or perceived offenses.

Mobile Providers Continue to be Reactive

There has been limited improvement in visibility and investment in detection/mitigation solutions specific to the mobile network since the last survey. The economics of consumer subscriber networks do not incent providers to implement security until a problem occurs.

Bring Your Own Device (BYOD) Trend Creates New Challenges

In the growing trend commonly referred to as BYOD, half of respondents now allow personal devices on their networks. However, only 40 percent have a means to monitor usage of these devices. Additionally, only 13 percent actively block access to social media applications and sites. Clearly, BYOD is creating more entry-points for hackers to enter the network.

More Bandwidth Available for More Users as Mobile Providers Rush to Deploy Long Term Evolution (LTE).

LTE deployments have significantly accelerated over the last two years. The advancing adoption of LTE deployments and wireless services in general, significantly increases the reach of broadband Internet access to a much larger user base. Additionally, it allows mobile devices to become the primary means of Internet access for users given the increased available bandwidth.

Much of the Internet’s DNS infrastructure Remains Open and Unprotected

Lack of dedicated security personnel and unrestricted recursive servers create an ideal environment for attackers to exploit.

IPv6 Deployments are Quickly Becoming Pervasive

Eighty percent of respondents have partial or full IPv6 deployments already in place with most using dual-stack as a migration mechanism. This opens new opportunities for attackers to bypass network controls by switching between IPv4 and IPv6 networks.

Demographics of Survey Respondents

This year, Arbor collected 130 responses from a mixture of Tier 1, Tier 2/3, enterprise and other types of network operators from all around the world. This represents a 14 percent increase over last year's 114 responses.

The mix of organizations responding to this year's survey showed a decrease in the proportion who classify themselves as Tier 2/3 operators, along with a decrease in the proportion of hosting/data center and co-location service providers. However, there was a large increase in the proportion of enterprise respondents (Figure 1).

Survey Respondents by Organizational Type

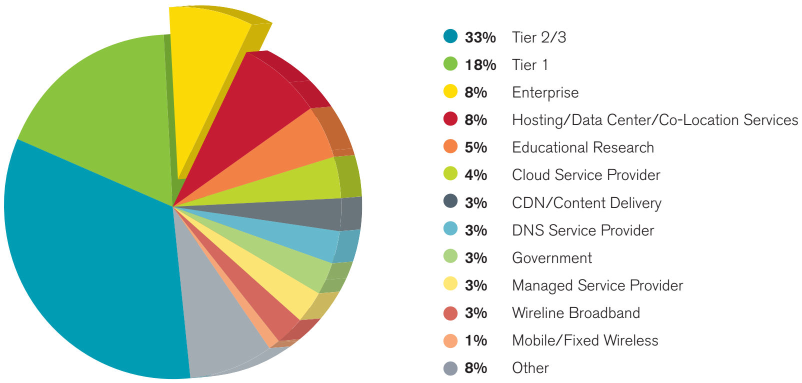


Figure 1 *Source: Arbor Networks, Inc.*

This year, the survey also queried the services offered by participating network operators (Figure 2). Most operators offer multiple services, with the most common being business Internet access, hosting co-location and DNS services. Thirty-two percent of our respondents offer managed security services, emphasizing the strength of the value-added services market. The "Other" category included WAN/VPN service providers, disaster recovery specialists and online auction platforms.

Services Offered (Non-Enterprise)

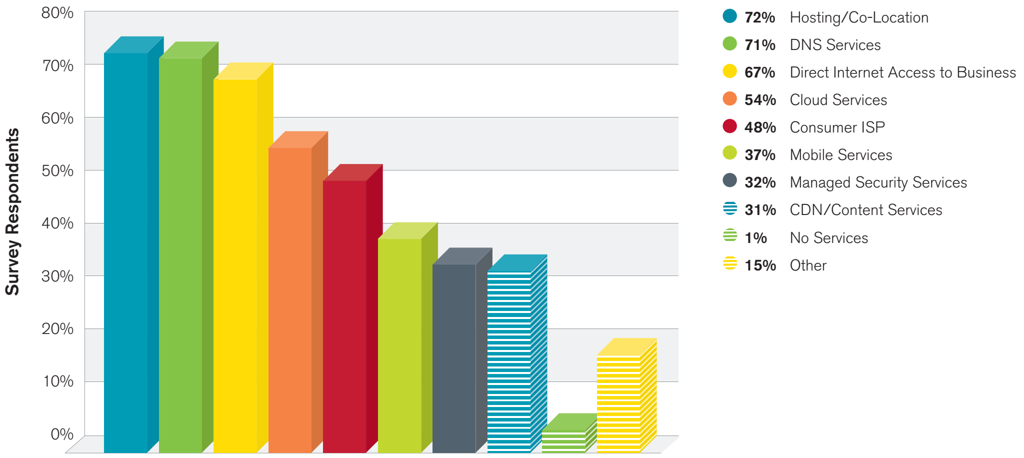


Figure 2 *Source: Arbor Networks, Inc.*

Network operators who participated in the survey were distributed all around the world (Figure 3). This distribution is very similar to that of last year's survey. The networks operated by the survey respondents often cover multiple regions. The proportion of respondents offering coverage in each region can be seen in Figure 4; again, this is consistent with the results from last year's survey.

Geographic Distribution of Organizational Headquarters

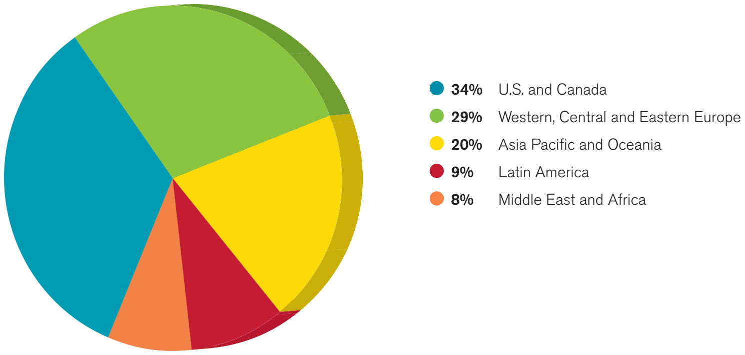


Figure 3 *Source: Arbor Networks, Inc.*

Geographic Coverage of Respondent Network

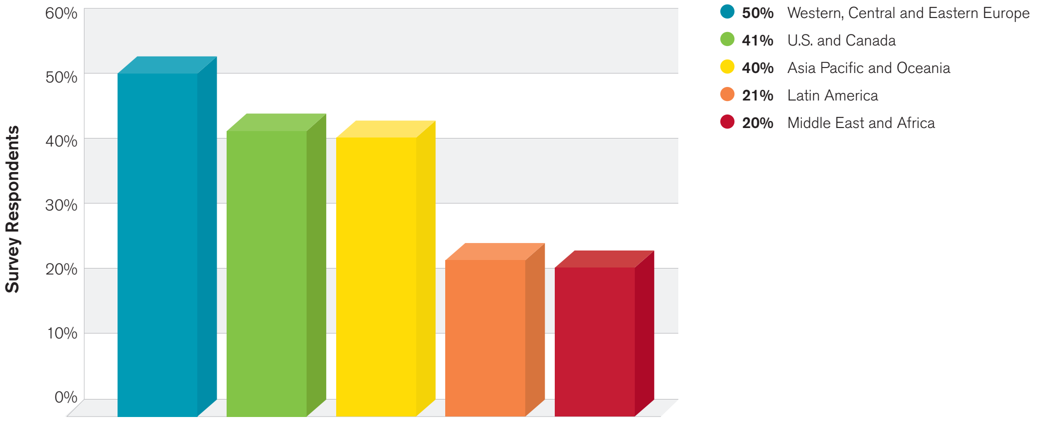


Figure 4 *Source: Arbor Networks, Inc.*

The majority of survey respondents are network or security engineers who are involved directly in day-to-day operational security issues (Figure 5). This year, a higher proportion of responses were from senior managers—15 percent more than last year—providing a broader view of the business implications of the security threats organizations face. The "Other" category included CISOs, organization/group technical officers and product marketing managers for security services.

Role of Respondent

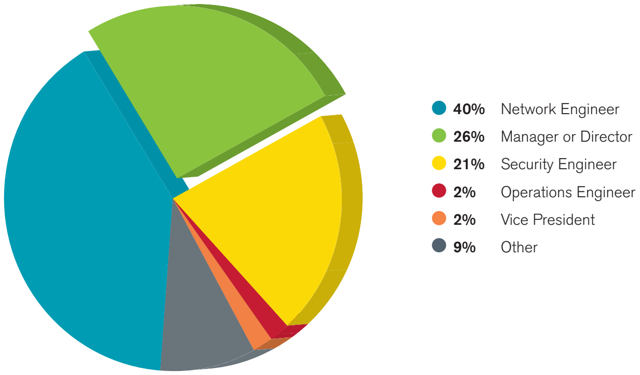


Figure 5 *Source: Arbor Networks, Inc.*

The majority of respondents work within small security operations teams. A concerning trend is that only 78 percent of respondents indicated that their organization has dedicated operational security resources—a decrease from last year. This may be a factor of OPEX reduction initiatives, or it could be an indication that more organizations are out-sourcing their security operations. It may also be related to the absorption of the security function into the networking function at organizations today. The proportion of respondent organizations having less than 10 dedicated operational security resources now stands at 71 percent, roughly the same as in last year's survey (Figure 6).

The key challenges facing respondents when building and maintaining an effective operational security team (Figure 7) were a "lack of headcount and resources" and "difficulty in finding and retaining skilled personnel." However, lack of both operating expense budget and capital funding were cited as issues by more of our respondents than in previous years, potentially indicating that cost reductions within network operations have had an impact here.

OPSEC Team Headcount

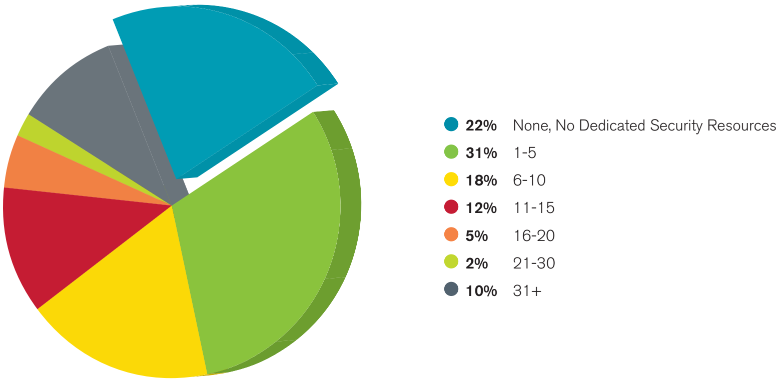


Figure 6 *Source: Arbor Networks, Inc.*

OPSEC Team Challenges

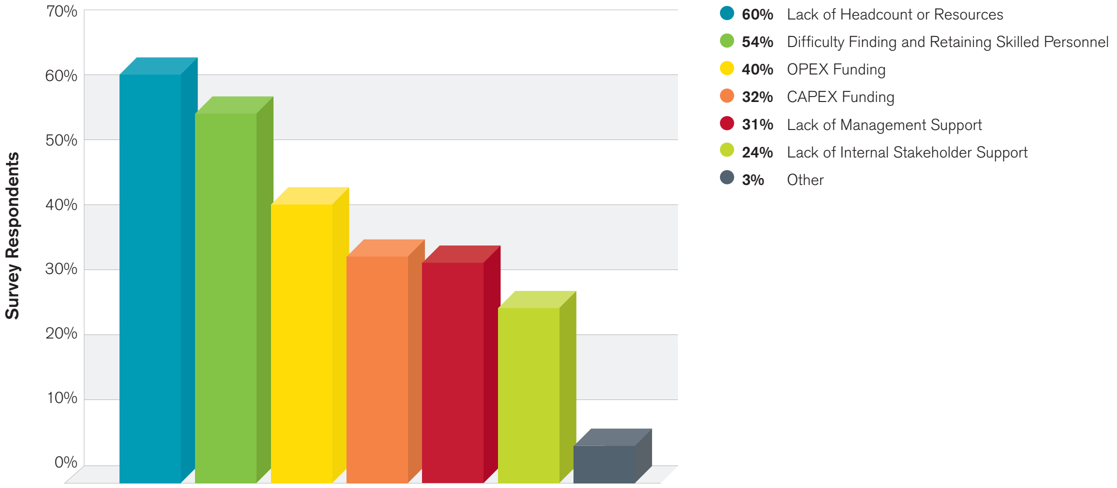
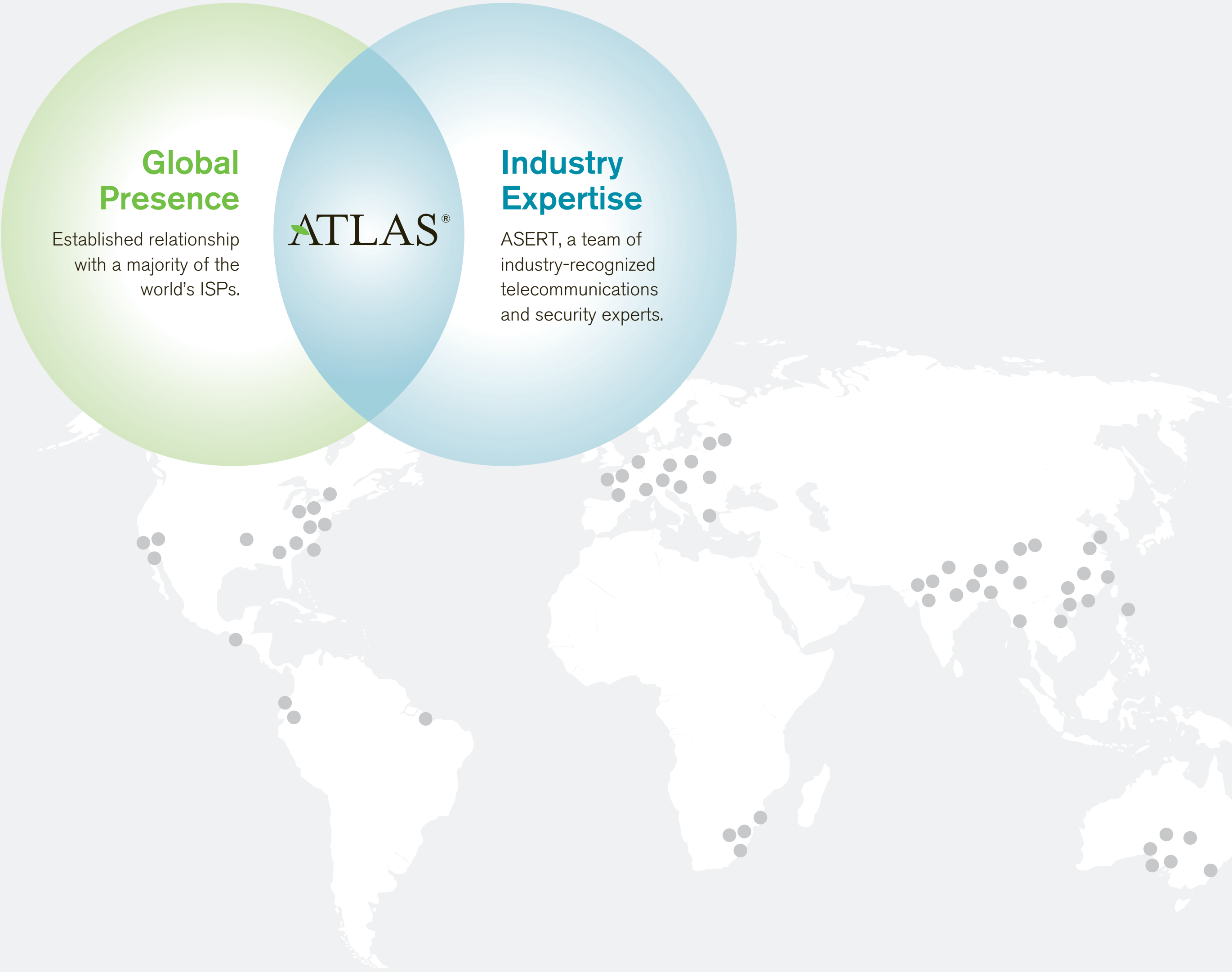


Figure 7 *Source: Arbor Networks, Inc.*

ATLAS® Introduction

For the first time, we are incorporating data in this report from Arbor's Active Threat Level Analysis System (ATLAS®). ATLAS is unique, as it is the only globally scoped threat analysis system in existence. ATLAS leverages Arbor's service provider customer base, the Arbor Security Engineering & Response Team (ASERT) and relationships with other organizations in the security community to collate and correlate information pertaining to current security threats.



Global Presence

Established relationship with a majority of the world's ISPs.

Industry Expertise

ASERT, a team of industry-recognized telecommunications and security experts.

This report makes use of ATLAS data for comparison/correlation with survey responses. ATLAS data relies upon (at time of writing) 250 Peakflow® SP customers from around the world anonymously sharing data on an hourly basis (Figures 8 and 9). The data shared includes information on the traffic crossing the boundaries of the participating network operators, and anonymized information on the DDoS attacks they are seeing crossing their network and targeting both their and their customers' infrastructure. The received data is collated and trended to deliver a detailed picture of the way in which DDoS attacks are evolving.

ATLAS Participants: Geographic Distribution

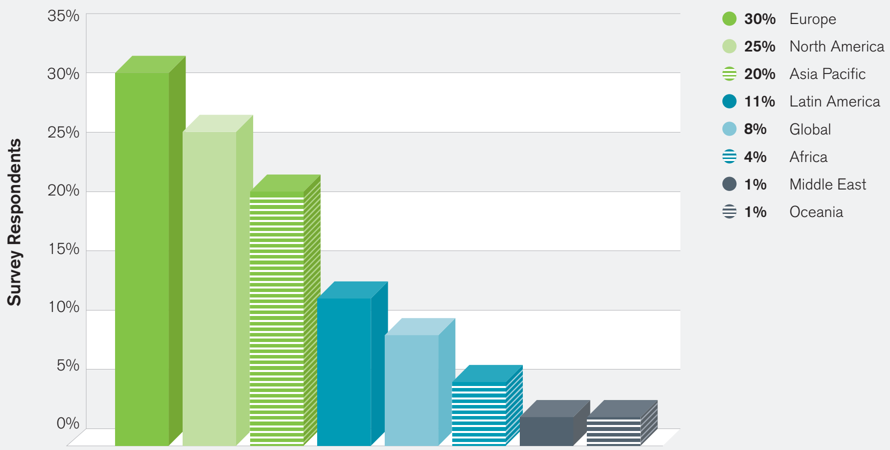


Figure 8 *Source: Arbor Networks, Inc.*

ATLAS Participants: Operator Type

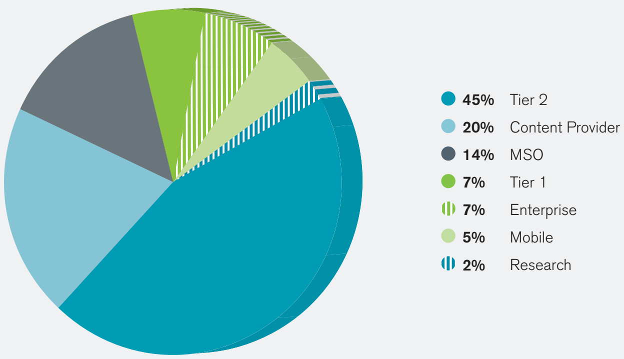


Figure 9 *Source: Arbor Networks, Inc.*

Most Significant Operational Threats

DDoS attacks against customers remain the number one operational threat or concern for survey respondents. Over half of respondents reported a higher level of awareness of the DDoS threat across their own and their customers' organizations.

Over three-quarters of survey participants experienced DDoS attacks toward their customers within the survey period (Figure 10). Over half reported seeing DDoS attacks against Internet services (DNS, email, etc.) and network infrastructure (routers, switches, load balancers, etc.)—a significant increase over last year.

Just under half of all respondents saw actual infrastructure outages due to DDoS. This clearly illustrates the threat DDoS attacks pose to Internet service availability and demonstrates the disparity in defense capabilities that Internet operators have available.

The second highest threat experienced in the last 12 months was outage due to failure or misconfiguration. This has been consistently experienced by 60 percent of survey respondents for the last three years, indicating that this problem does not appear to be going away or improving substantially.

Most Significant Operational Threats Experienced

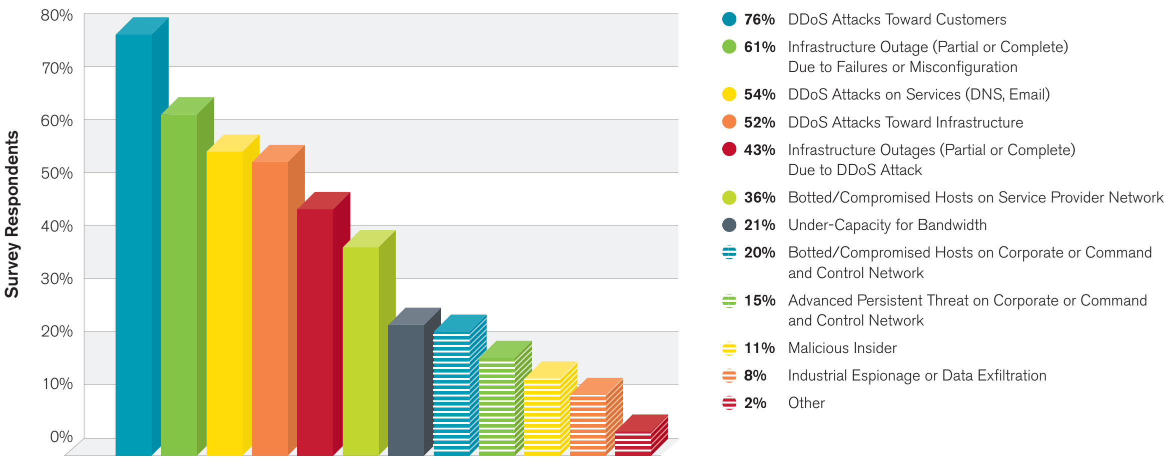


Figure 10 *Source: Arbor Networks, Inc.*

Over the next 12 months, DDoS attacks represent the top four concerns, the same result as last year, with attacks against customers being the top concern (Figure 11). Interestingly, outages due to failure or misconfiguration are the first non-DDoS-related concern, ranked fifth, even though they have consistently been the second most commonly experienced threat over the past three years.

Advanced persistent threat (APT) is a concern for more than a quarter of respondents. And, there is an increased level of concern over botted or compromised machines on service provider networks. This may indicate that infected hosts are causing problems for operators.

Operational Security Concerns in the Next 12 Months

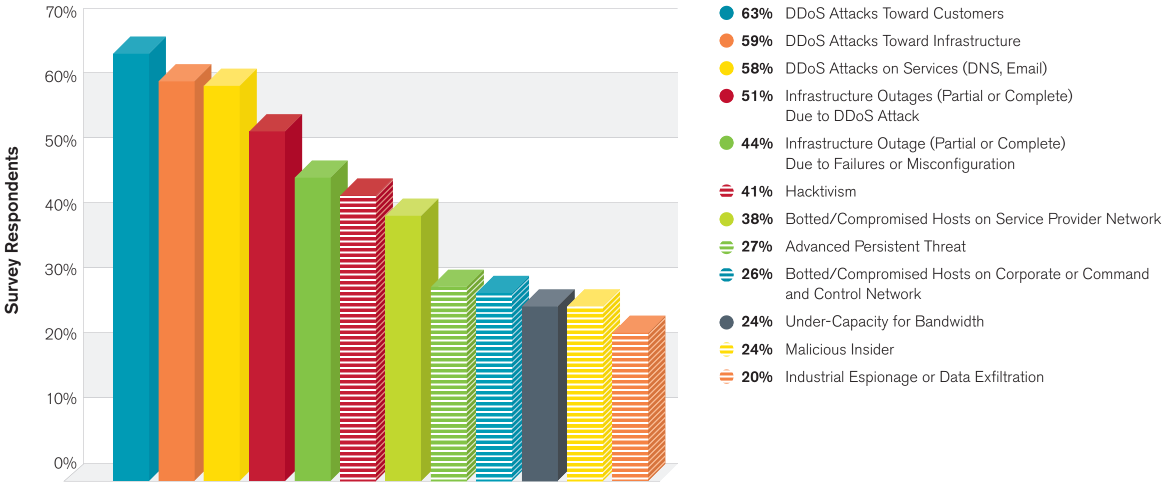


Figure 11 *Source: Arbor Networks, Inc.*

Seventy percent of survey respondents indicated that geographic sources of traffic influence their perception of the potential for threat. However, under half of respondents anticipated an actual rise in state-sponsored attacks during the next year.

The overall level of DDoS awareness continues to rise with over half of respondents reporting that their organization and their customers' organizations have a higher level of awareness than they did last year (Figures 12, 13, 14 and 15). Much of the awareness comes the hard way with respondents' networks and their customers experiencing attacks, but a number are now paying attention to the highly publicized attacks in the news and are acting proactively. Even more encouraging, over 30 percent of respondents now include DDoS within their business continuity and risk management strategies.

Level of DDoS Threat Awareness in Respondents' Organizations

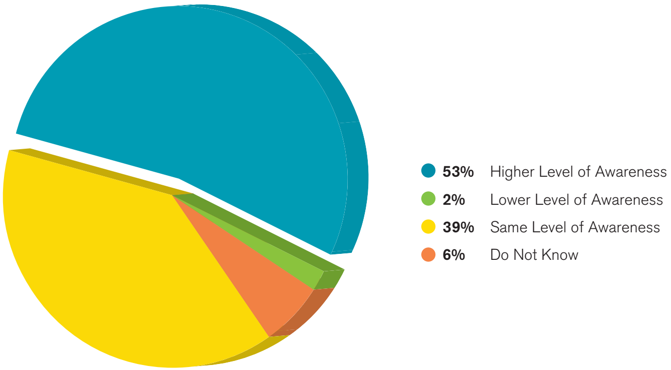


Figure 12 *Source: Arbor Networks, Inc.*

Level of DDoS Threat Awareness in Respondents' Customer Organizations

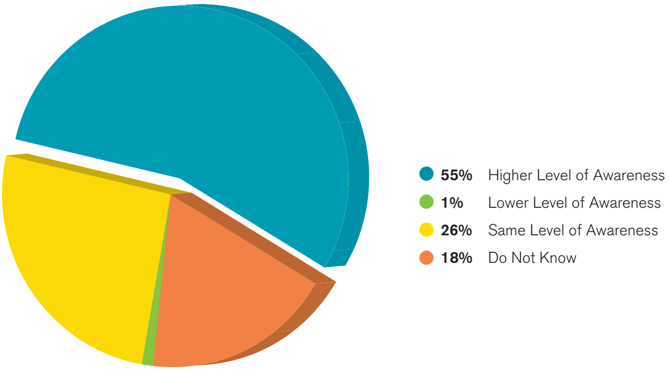


Figure 13 *Source: Arbor Networks, Inc.*

Factors Influencing Higher Level of DDoS Awareness in Respondents

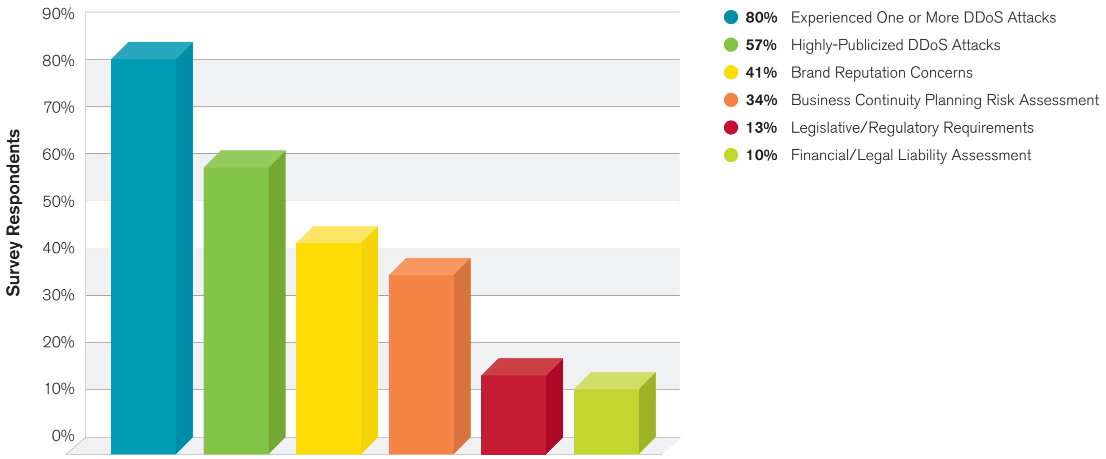


Figure 14 Source: Arbor Networks, Inc.

Factors Influencing Higher Level of DDoS Awareness in Respondents' Customers

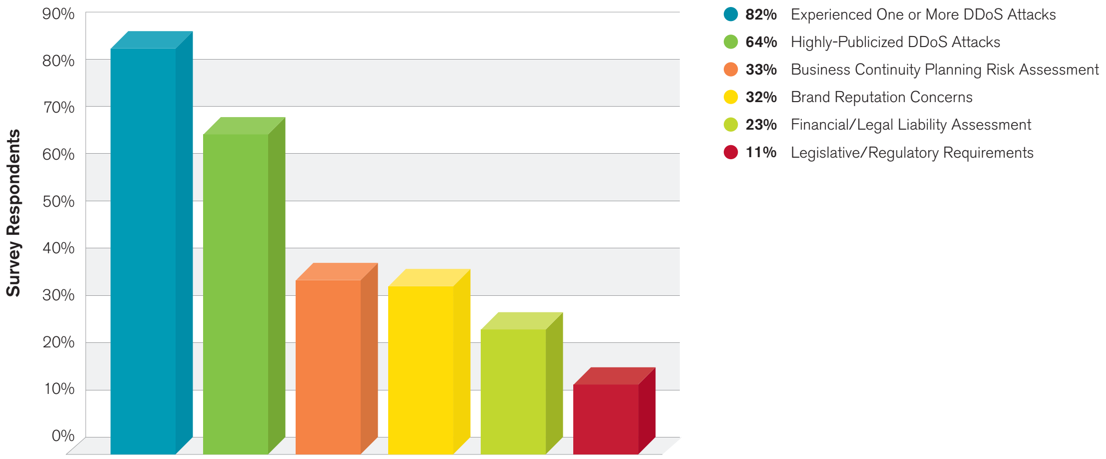


Figure 15 Source: Arbor Networks, Inc.

Motivation, Scale, Targeting and Frequency of DDoS Attacks

As expected, ideological hacktivism was again perceived as the most common motivation behind the DDoS attacks monitored by our survey respondents. The largest attack reported was 60 Gbps, identical to last year's survey, with end users being the most common targets for the largest monitored attacks.

Taking the common or very common motivations perceived by our survey respondents, ideological hacktivism kept its number one position from last year (Figure 16), with the number two and three motivations—online gaming-related and nihilism/vandalism—switching places. It is important to consider the fact that all three of the top motivations for attacks have an emotional component to them that makes them very unpredictable. Perceived slights between individuals or between individuals and companies have now become a major root cause of DDoS attacks. It should also be noted that although many of the attacks reported in the media tend to be ideologically motivated, many other attacks do take place with alternate motivations. As survey results show, approximately 15 percent of respondents see attacks commonly or very commonly motivated by extortion, competitive rivalry between organizations or as a distraction from data theft.

Most Common Motivations Behind DDoS Attacks

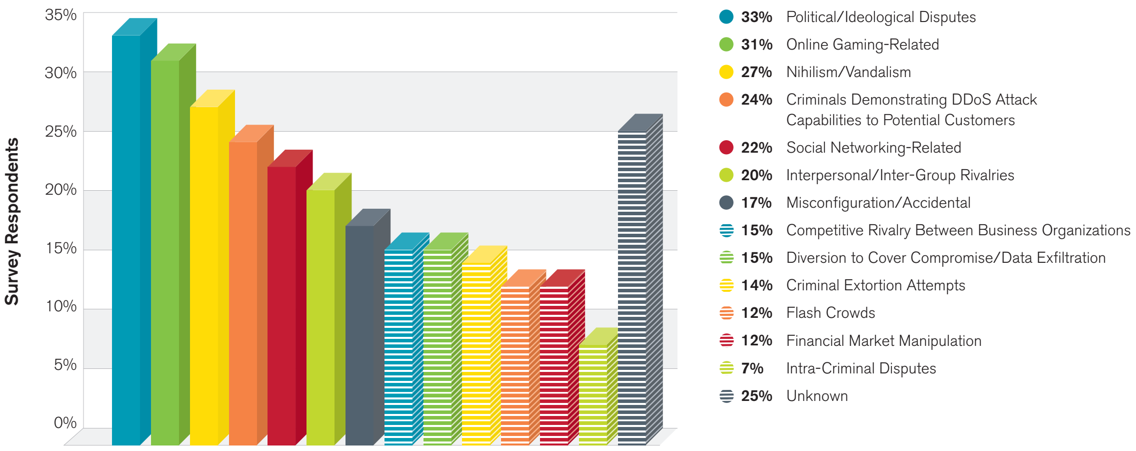


***Figure 16** Source: Arbor Networks, Inc.*

ATLAS-Monitored Attacks Sizes

As mentioned earlier in this report, the ATLAS system gathers statistics from 250 participating network operators around the world. These statistics include anonymized details of the DDoS attacks monitored by participants.

This rich dataset is then collated and analyzed by the ASERT team. Using this dataset, Arbor can derive the peak attack sizes seen across the Internet—hour-by-hour, day-by-day and month-by-month. The largest attacks tracked by survey respondents appear to have decreased from their 2010 high of 100 Gbps, to 60 Gbps in both 2011 and 2012; however, ATLAS is still tracking attacks at around the 100 Gbps level (Figure 17). Average tracked attack sizes have continued to grow over the past 12 months. Average attacks are now consistently above 1 Gbps, month-by-month (Figure 18). This is relevant given the prevalence of 1 Gbps (and lower) Internet connectivity, as average attacks are now capable of saturating these links.

ATLAS Peak Monitored Attack Sizes Month-By-Month (January 2009-Present)

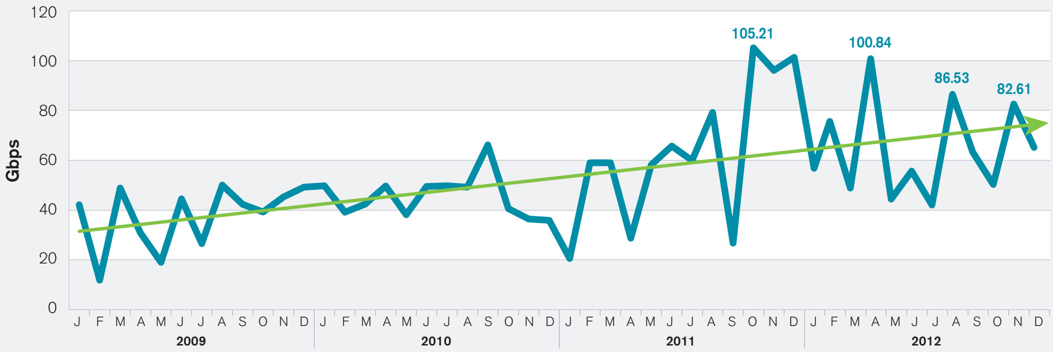


Figure 17 *Source: Arbor Networks, Inc.*

ATLAS Average Monitored Attack Sizes Month-By-Month (January 2009-Present)

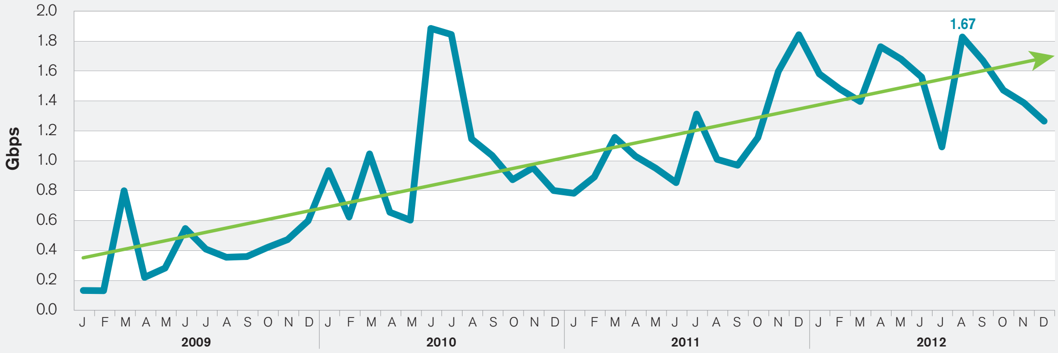


Figure 18 *Source: Arbor Networks, Inc.*

The largest attack reported by our survey respondents during the survey period was 60 Gbps (Figure 19). This attack targeted the DNS infrastructure of the respondent operator in order to impact a specific customer served by that infrastructure. The largest attack reported last year was the same size (60 Gbps), a reduction from the 100 Gbps largest attack reported in 2010. Despite the survey results, larger attacks are still happening, but the largest attacks recorded do appear to have plateaued at around 100 Gbps. This is a very significant volume of traffic and is more bandwidth than some Internet operators have, let alone their customers. It also indicates that attackers are shifting to more advanced blended threat approaches.

Some comments from respondents on "largest monitored attacks" include:

- "Sustained attack for 5 Gbps for about 4 hours. UDP flood of sourced from random ports destined to random ports of the target resource."
- "Covering DDoS for a web infiltration attempt. 7.3 Gbps on the website, then on the network analyzer, then back on the website. Under was a set of web compromise attacks."
- "TCP/80 SYN flood toward Chinese online gaming (not gambling) site who was a DDoS mitigation customer of ours. Motivations unknown. Frequent on-and-off waves of attack traffic over several days, the largest of which topped out at 28.3 Mpps."
- "DDoS attack, UDP flood toward online gaming server."
- "UDP reflection/amplification attack, primarily a mix of port 53 and 520 with some SYN and ICMP backscatter. Suspected attack motivation was retaliatory attack to something our users posted on a web forum (destination of the attack was a web proxy)."
- "UDP port 22 small byte packets at high rate for less than 10 minutes, overran firewalls supposedly able to handle much higher pps rates."

Size of Largest Reported DDoS Attack (Gbps)

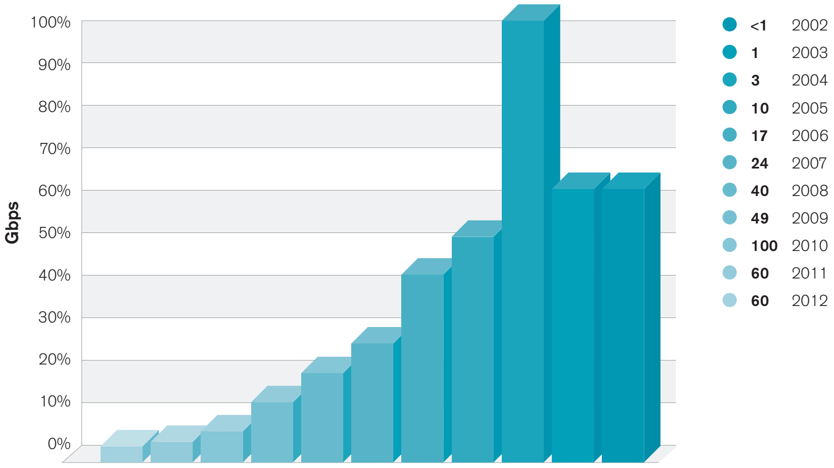


Figure 19 *Source: Arbor Networks, Inc.*

The overwhelming majority of respondents saw their largest attacks targeting their customers (Figure 20). This is consistent with last year's results.

Target of Largest DDoS Attack

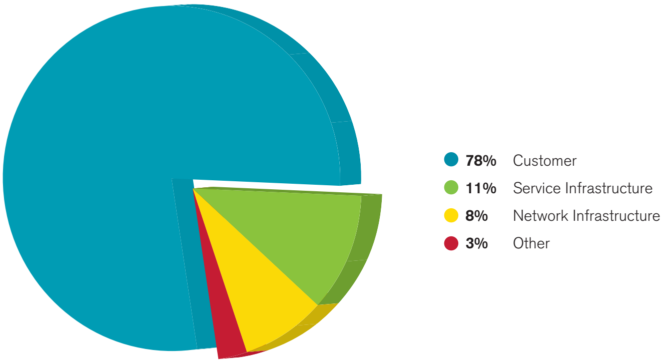


Figure 20 *Source: Arbor Networks, Inc.*

In general, customers of the survey's respondents are the most common targets of attack (Figure 21). Service infrastructure (DNS servers, email servers, Web portals, etc.) is the second most common target. This demonstrates a trend toward more focused attacks on end user organizations versus broad attacks on operator infrastructure.

Monitored Attack Targets

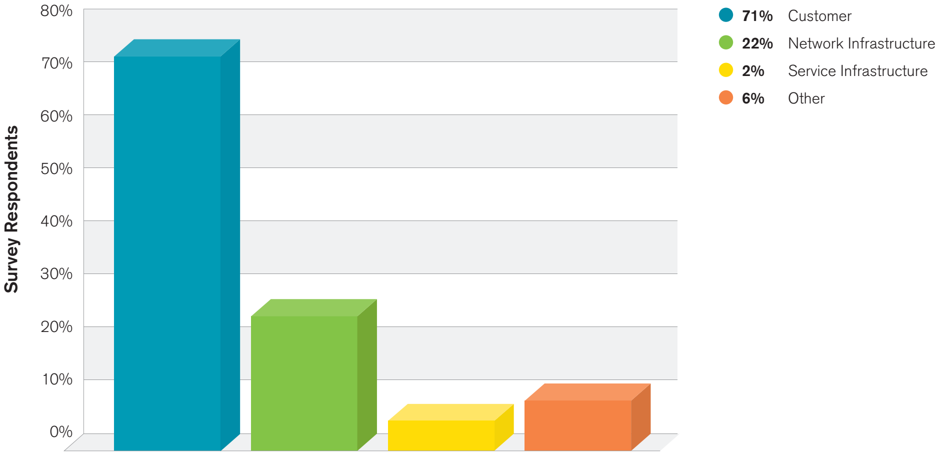


Figure 21 *Source: Arbor Networks, Inc.*

This year, the survey contained an additional question to gain some insight into the types of customers being targeted by DDoS attacks (Figure 22), the results of which are interesting. Based on Arbor's involvement in helping customers with attack mitigation, we would have anticipated that financial, e-commerce and government organizations are the most common targets. As you can see, e-commerce organizations were cited as the top target by nearly half the respondents, but surprisingly, the next largest target groups are end users/subscribers and gaming/gambling sites.

Targeted Customer Types

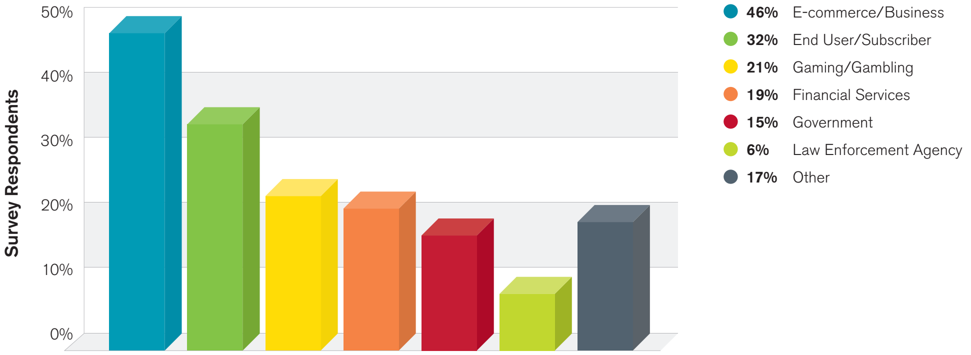


Figure 22 *Source: Arbor Networks, Inc.*

With the growing supply and use of cloud and NAT services by network operators, the survey asked our respondents some specific questions on whether they have seen this infrastructure being targeted by DDoS attacks. Only 14 percent of respondents have seen attacks targeting any form of cloud service, with just under one-third seeing attacks targeting NAT infrastructure. However, just over half of those who saw attacks targeting NAT did see a significant impact from an attack (Figure 23).

Impact of Attacks Against NAT Infrastructure

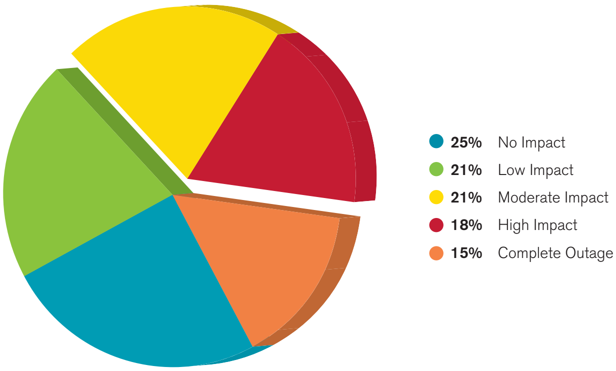


Figure 23 *Source: Arbor Networks, Inc.*

DDoS attack vectors vary significantly between attacks. Attack vectors tend to fall into one of three broad categories:

1. **Volumetric Attacks:** These attacks attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.
2. **TCP State-Exhaustion Attacks:** These attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls and the application servers themselves. Even high-capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.
3. **Application-Layer Attacks:** These target some aspect of an application or service at Layer 7. They are the most sophisticated, stealthy attacks because they can be very effective with as few as one attacking machine generating a low traffic rate. This makes these attacks very difficult to proactively detect and mitigate.

Within these categories, the actual attack vectors being used are evolving continuously, with new and more complex attack tools being produced by the hacker community all the time. Arbor's ASERT blog (ddos.arbornetworks.com) contains the latest analysis.

Application-layer attacks have become increasingly common over the past few years, with 86 percent of our respondents reporting application-layer attacks targeting Web services (Figure 24). Interestingly, the proportion of reported application-layer attacks has not changed much over the last few years for most services such as HTTP, DNS, SMTP, etc. The only clear change is in relation to HTTPS, with 37 percent of our respondents seeing application-layer attacks targeting this service—up from 24 percent last year. This may indicate that encrypted services, such as those used to check out of e-commerce sites and by financial service portals, are being targeted by application-layer attacks.

Targets of Application-Layer Attacks

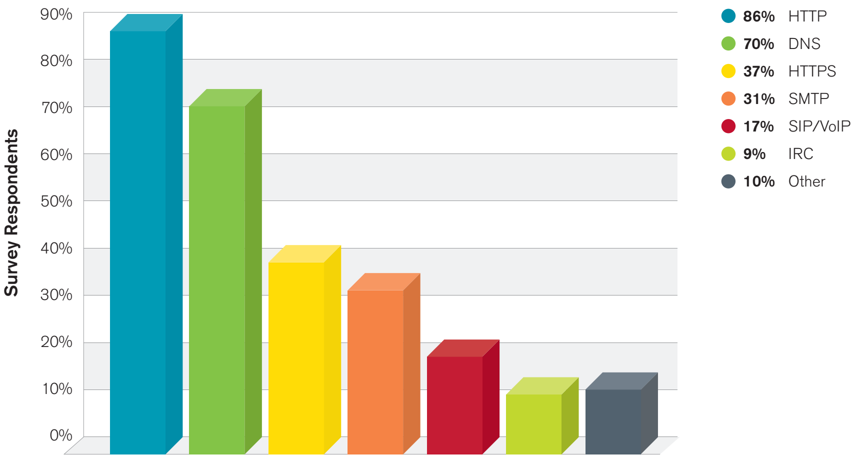


Figure 24 *Source: Arbor Networks, Inc.*

Looking at the attacks targeting encrypted services in more detail, it is worth noting that there is an approximate 50/50 split between respondents who saw the service running over the encrypted transport being targeted, and those who saw both the service and the underlying encryption protocol being targeted by attacks.

Web services remain the most popular targets for application-layer attacks, with respondents seeing a broad range of attack vectors being used (Figure 25). HTTP GET floods are the most common attack vector, with multiple malware variants and tools being capable of generating attacks of this kind. LOIC came in second place. At time of writing, LOIC has been downloaded 662,983 times since the start of 2012; it is a good illustration of how accessible some of these attack tools have become.

Application-Layer Attack Vectors Targeting Web Services

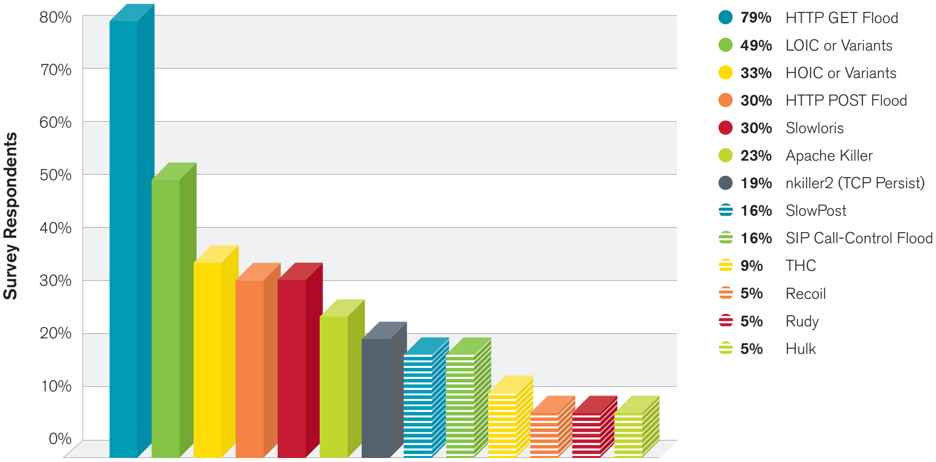


Figure 25 *Source: Arbor Networks, Inc.*

A very concerning statistic is the growth in the proportion of respondents reporting multi-vector DDoS attacks (Figure 26). These attacks involve combinations of volumetric, state-exhaustion and application-layer attack vectors targeting an organization at the same time. In last year's survey, 27 percent of respondents had experienced these attacks. This has increased to 46 percent this year. These attacks can be challenging to mitigate and generally require layered solutions across the data center and the cloud to manage.

Multi-Vector DDoS Attacks

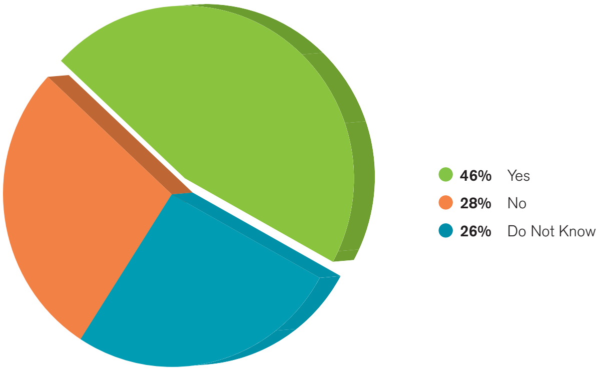


Figure 26 *Source: Arbor Networks, Inc.*

An Example of a Multi-Vector Attack in Action: ASERT

The following excerpt was originally published on the ASERT blog, ddos.arbornetworks.com.

During the fourth quarter of 2012, we witnessed a targeted, sophisticated campaign of DDoS attacks against U.S.-based financial institutions. These attacks were very much premeditated, focused, advertised before the fact, and executed in a coordinated and organized manner.

In the case of the Q4 2012 DDoS attack campaign targeting US financial institutions, many compromised PHP Web applications were used as bots in the attacks. Additionally, many WordPress sites, often using the out-of-date TimThumb plug-in, were being compromised around the same time. Joomla and other PHP-based applications were also compromised. Unmaintained sites running out-of-date extensions are easy targets, and the attackers took full advantage of this to upload various PHP webshells that were then used to further deploy attack tools. Attackers connect to the compromised Web servers hosting the tools directly or through intermediate servers/proxies/scripts and issue attack commands. These attacks used several PHP-based tools. The most prominent was “Brobot.” Two other tools, KamiKaze and AMOS, were used a bit less often. Brobot has also been referred to as “itsoknoproblembro.”

The attack tactics observed were a mix of application-layer attacks on HTTP, HTTPS and DNS with volumetric attack traffic on a variety of TCP, UDP, ICMP and other IP protocols. The other obvious and uncommon factor at play was the launch of simultaneous attacks, at high bandwidth, to multiple companies in the same vertical.

On December 10, 2012, the group claiming responsibility for the prior attacks, the Izz ad-Din al-Qassam Cyber Fighters, announced “Phase 2 Operation Ababil.” A new wave of attacks was announced on their Pastebin page.

On December 11, 2012, attacks on several of the pre-announced targets were observed. Some attacks looked similar in construction to Brobot v1. However, there is a newly crafted DNS packet attack and a few other attack changes in Brobot v2.

These attacks have shown why DDoS continues to be such a popular and effective attack vector. Yes, DDoS can take the form of very large attacks. In fact, some of these attacks have been as large as 60 Gbps. What makes these attacks so significant is not their size, but the fact that the attacks are quite focused, part of an ongoing campaign, and like most DDoS attacks, quite public. These attacks utilize multiple targets, from network infrastructure to Web applications.

Continued on page 26

An Example of a Multi-Vector Attack in Action: ASERT (continued)

Lessons Learned

While there has been much speculation about who was behind these attacks, our focus is less on the "who" or "why," but how we can successfully defend going forward. Multiple lessons can be learned from these attacks by everyone involved—the targeted enterprises, their managed security providers, Web site and Web application administrators and the vendor community.

For enterprises, it is clear that typical perimeter defenses such as firewalls and IPS are not effective when dealing with DDoS attacks, as each technology inline to the target is a potential bottleneck. These devices can be an important part of a layered defense strategy, but they were built for problems far different than today's complex DDoS threat. Given the complexity of today's threat landscape and the nature of application-layer attacks, it is increasingly clear that enterprises need better visibility and control over their networks, which require a purpose-built, on-premise DDoS mitigation solution. This could sound self-serving. However, visibility into a DDoS attack needs to be far better than the first report of your Web site or critical business asset going down. Without real-time knowledge of the attack, defense and recovery become increasingly difficult.

Providers of managed security services have begun to evaluate their deployments and mitigation capacity. These attacks were unique in that they targeted multiple organizations within the same vertical, putting a strain on the capacity of a provider's cloud-based mitigation services.

What these attacks have continued to demonstrate is that DDoS will continue to be a popular and increasingly complex attack vector. DDoS is no longer simply a network issue, but is increasingly a feature or additional aspect of other threats.
The motivation of modern attackers can be singular, but the threat landscape continues to become more complex and mixes various threats to increase the likelihood of success. There have certainly been cases where the MSSP was successful at mitigating against an attack, but the target Web site still went down due to corruption of the underlying application and data. To defend networks today, enterprises need to deploy DDoS security in multiple layers, from the perimeter of their network to the provider cloud, and ensure that on-premise equipment can work in harmony with provider networks for effective and robust attack mitigation.

The proportion of respondents seeing between one and 20 attacks per month is now at just over 70 percent (Figure 27), up from around 60 percent last year. Overall, attack frequencies are fairly similar to last year, with a decrease in the proportion of respondents reporting between 100 and 500 attacks per month.

Attack Frequency per Month

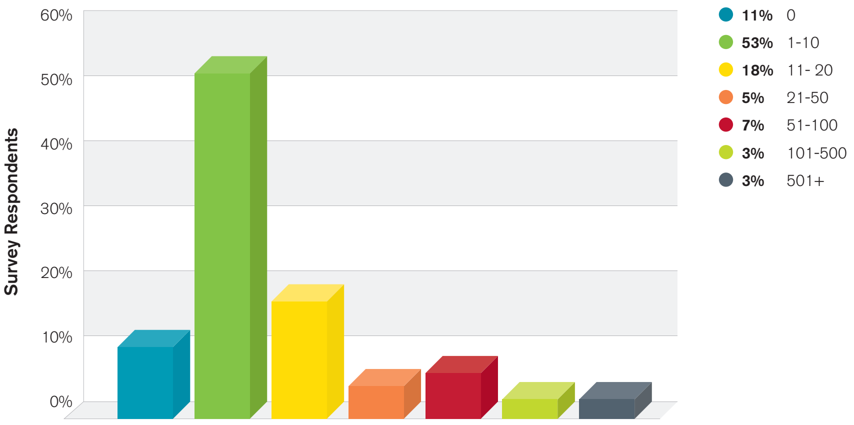


Figure 27 *Source: Arbor Networks, Inc.*

The durations of the longest attacks reported were quite varied (Figure 28). One-third of respondents indicated that the longest attacks they witnessed were less than six hours in duration, with 38 percent reporting their longest attacks lasting between one and seven days.

Longest Attack Duration

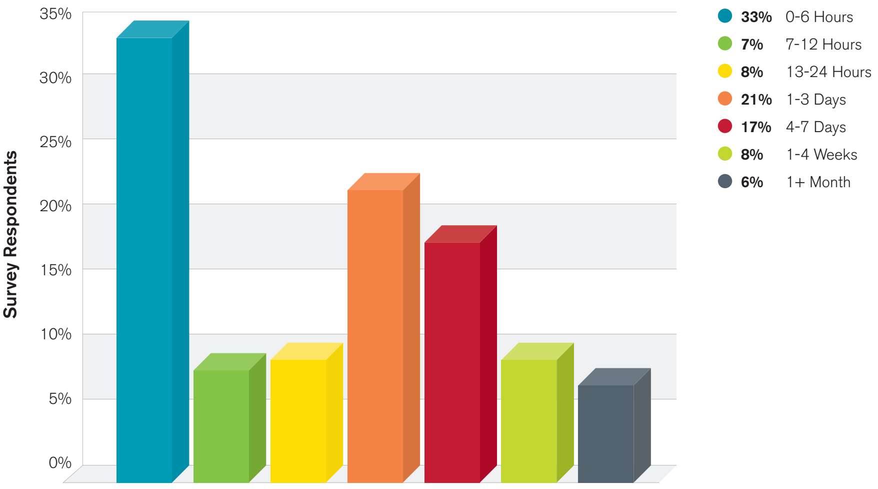


Figure 28 *Source: Arbor Networks, Inc.*

ATLAS-Monitored Attack Durations

In addition to tracking attack sizes, ATLAS also allows Arbor to track the duration of attacks monitored by the 250 participating network operators. At the time of this writing, the "average" duration of a monitored attack in 2012 stands at 3 hours and 46 minutes.

The distribution of attack durations is wide (Figure 29), with 77 percent of individual attacks currently lasting less than one hour.

ATLAS-Monitored Attack Duration

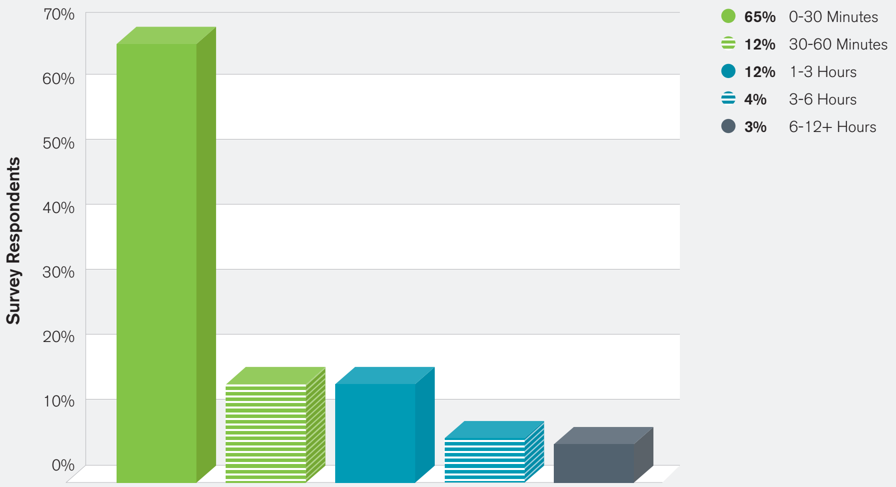


Figure 29 *Source: Arbor Networks, Inc.*

Network, Customer and Service Threat Detection

Firewall, IDS and commercial IP flow processing systems are the most commonly used threat detection mechanisms. However, the combined proportion of respondents using either commercial and/or open-source flow tools for threat detection stands at 91 percent.

This year, the questions in the survey regarding threat detection were broadened to cover “threats targeting networks, customers or services” rather than specifying purely DDoS attacks as in previous surveys. Firewalls and IDS systems were the most commonly used threat detection mechanisms, marginally ahead of commercial flow processing systems, with in-house developed scripts/tools in third place (Figure 30).

Threat Detection Tools Utilized

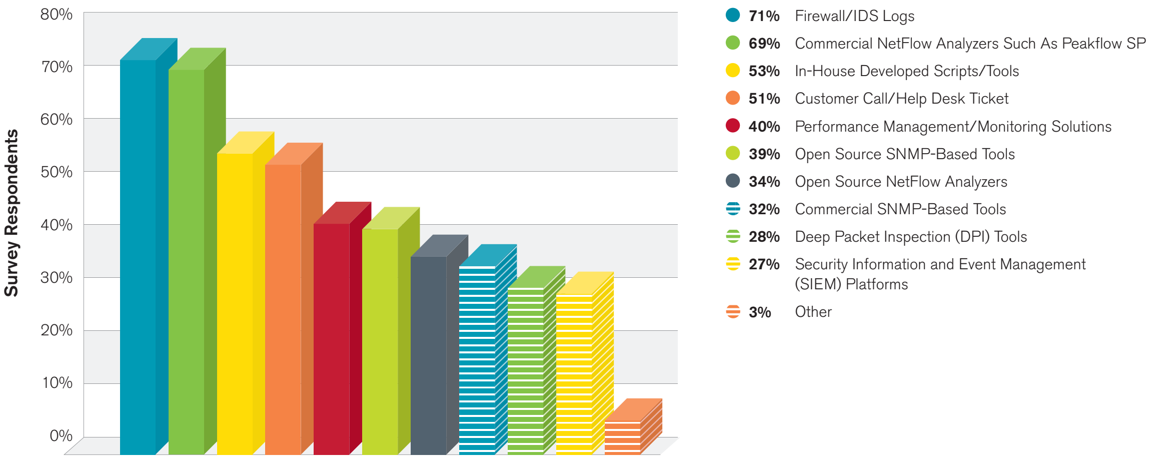


***Figure 30** Source: Arbor Networks, Inc.*

It is concerning that over half of respondents report using customer calls or help desk tickets as a threat detection mechanism, as this is a completely reactive approach ensuring slow response. Ninety-one percent of respondents use some type of flow telemetry for threat detection. This is encouraging as flow telemetry provides a scalable and non-invasive way of monitoring a network.

Flow export technologies commonly only incorporate Layer 3 and Layer 4 data. This can make the proactive detection of some stealthy application-layer threats difficult. Some network equipment vendors are now incorporating Layer 7 information within flow. Just over a quarter of our respondents are already utilizing this, with another 37 percent reporting that they would desire to implement it, but do not have support for this functionality within their infrastructure (Figure 31).

Collection of Layer 7 Information Within Flow Export

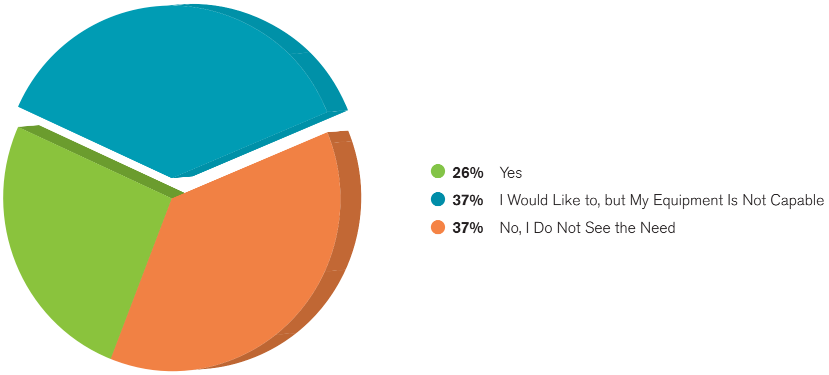


Figure 31 *Source: Arbor Networks, Inc.*

Only 51 percent of respondents now detect outbound/cross-bound DDoS attacks. This continues a trend, down 6 percent from last year and 22 percent from the year before. It appears that our respondents may perceive outbound attacks as less important than attacks targeting their infrastructure and customers. It should be noted that outbound attacks consume capacity, can affect peering ratios and can also result in SLA and billing disputes with end users.

Last year was the first where respondents had detected and reported attacks against IPv6 services, with 4 percent doing so. This year, the proportion of respondents reporting attacks against IPv6 services has fallen to less than 3 percent. This demonstrates the relatively slow rate of IPv6 market penetration, even with events like World IPv6 Launch increasing the availability of services. We believe that the number and impact of these attacks will increase as more services are available over IPv6 and more end users access the Internet using IPv6.

Attack Mitigation Techniques

ACLs remain the most popular DDoS attack mitigation mechanism, despite their functional and operational limitations. However, there has been a rise in the proportion of respondents using Intelligent DDoS Mitigation Systems (IDMS) to protect their customers and services.

The percentage of respondents utilizing ACLs for DDoS mitigation has remained almost equal to that reported in last year's survey (Figure 32). However, there has been a substantial increase in the proportion of respondents using IDMS to mitigate attacks, up from 45 percent to 60 percent. This is encouraging as IDMS solutions, and the services based on them, are specifically designed to deal with the DDoS threat and offer the best protection for end user organizations and network operators.

Attack Mitigation Techniques

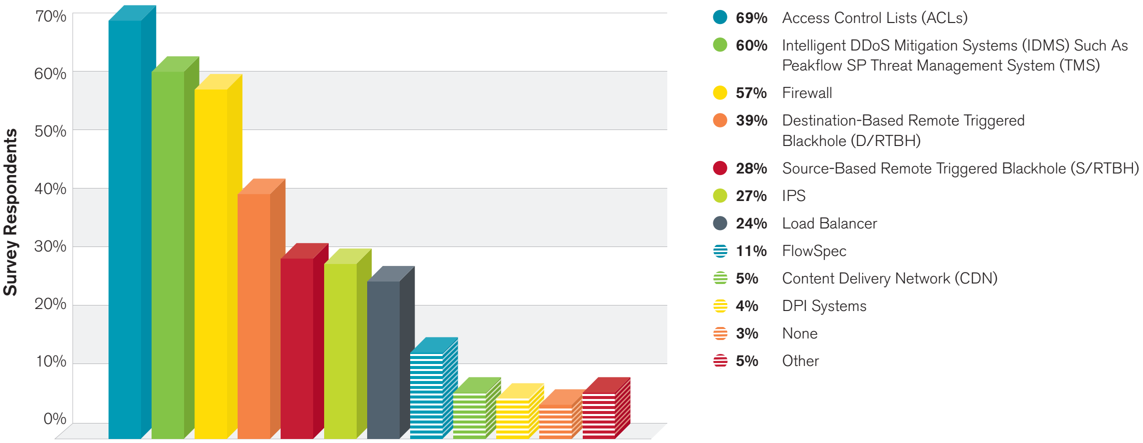


__Figure 32__ Source: Arbor Networks, Inc.

However, a big concern is the reported increase in the use of firewalls for DDoS mitigation, up from just over one-third of respondents last year to 57 percent this year. As has been discussed in previous iterations of this report, firewalls are not designed to deal with DDoS attacks. In fact, their reliance on maintaining session state can make them being the targets of some state-exhaustion attacks (or they can be impacted due to state exhaustion as attack traffic passes through them). Firewalls can be used to mitigate some DDoS attacks, and are an essential part of a layered-security model, but relying on them to deal with large, complex DDoS attacks can put service availability at risk.

Encouraging is the drop in the proportion of respondents using destination based remote triggered black-hole (D-RTBH) as a mitigation mechanism—from just over half of respondents to 39 percent. D-RTBH drops all traffic toward the victim of an attack, protecting other network operator customers and services from collateral damage. This is obviously not an ideal solution for the original target, as the attack is effectively completed. The reduction in the proportion of respondents using D-RTBH drop may indicate that operators are starting to use alternatives such as IDMS to protect their customers from attacks, maintaining service availability.

More than half of respondents are now able to mitigate attacks within 20 minutes, a small improvement over last year's results (Figure 33). The percentage of respondents taking 30 minutes or more has fallen from 33 percent to 25 percent. This indicates that operators are now able to deal more quickly with more complex application-layer attack vectors—possibly due to increased experience or more automated features in mitigation products.

Time to Mitigate Attacks

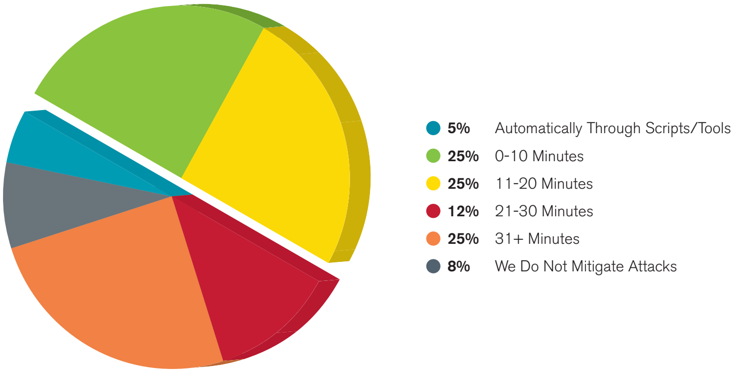


Figure 33 *Source: Arbor Networks, Inc.*

Looking at the mitigation of outbound attacks, just under one-third of our respondents indicated that they do not have mechanisms in place to do this. For those who do, ACLs are used by nearly half of respondents, with firewalls in second place (Figure 34). This is an almost identical set of results to last year. Although two-thirds of our respondents have mechanisms in place to mitigate outbound DDoS attacks, only one-third actually mitigated an outbound attack during the survey period.

Outbound Attack Mitigation Techniques

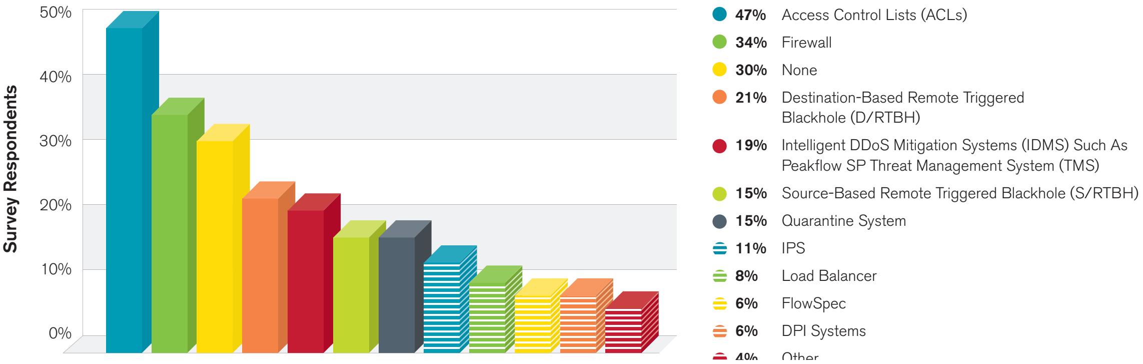


Figure 34 *Source: Arbor Networks, Inc.*

IPv6 Observations

IPv6 deployments continue with dual-stack being the most common migration strategy. Visibility of IPv6 traffic is still important to respondents, with more having either full or partial support for flow telemetry from their infrastructure. However, only half of respondents have an IPv6 visibility solution in place.

This year, nearly 80 percent of our respondents indicated that they either have already deployed IPv6 or have plans to deploy within the next 12 months. Of those, just under one-quarter have completed their deployment of IPv6, with a further 54 percent in process. The rest are planning a deployment soon (Figure 35).

IPv6 Deployment Progress

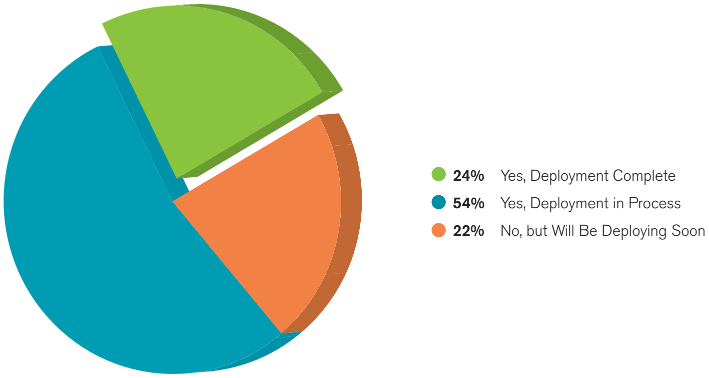


Figure 35 *Source: Arbor Networks, Inc.*

As in the last two years' surveys, 57 percent of respondents indicated that IPv4 address availability was not an issue for them, and would not be within the next 12 months. This may well be due to the fact that the majority of respondents already have migration plans for IPv6 in place.

In terms of migration strategies (Figure 36), over 90 percent of respondents have opted for dual-stack deployments; however, a percentage of them are planning on using tunneling and/or address translation, which may increase their threat surface.

IPv6 Migration Strategy

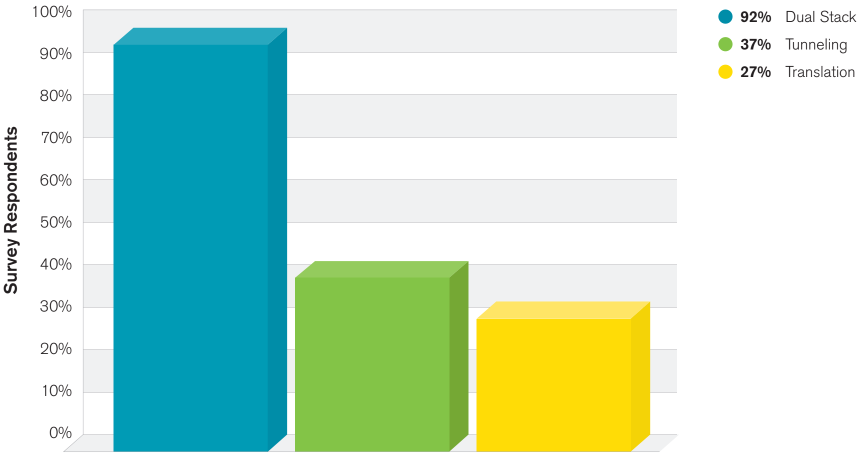


Figure 36 *Source: Arbor Networks, Inc.*

As in previous iterations of this report, the majority of respondents indicated that getting visibility into the IPv6 traffic on their network is critical for them (Figure 37). However, only one-half of respondents actually have a visibility solution for IPv6 traffic deployed.

Criticality of IPv6 Traffic Visibility

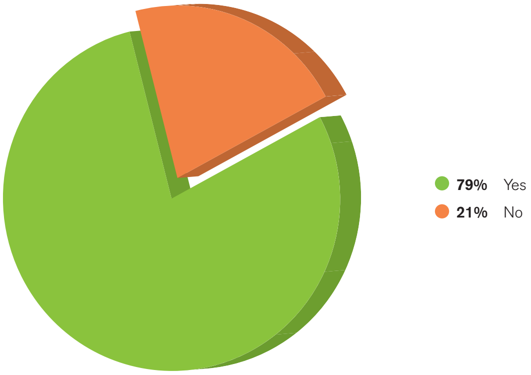


Figure 37 *Source: Arbor Networks, Inc.*

This year's results show a clear increase in the proportion of respondents who have either partial or full support for IPv6 flow telemetry from their network infrastructure (Figure 38)—an increase from 63 percent last year to 74 percent this year. Flow telemetry is very important for scalable, cost-effective threat detection and visibility, so this change is very positive.

IPv6 Flow Telemetry Support

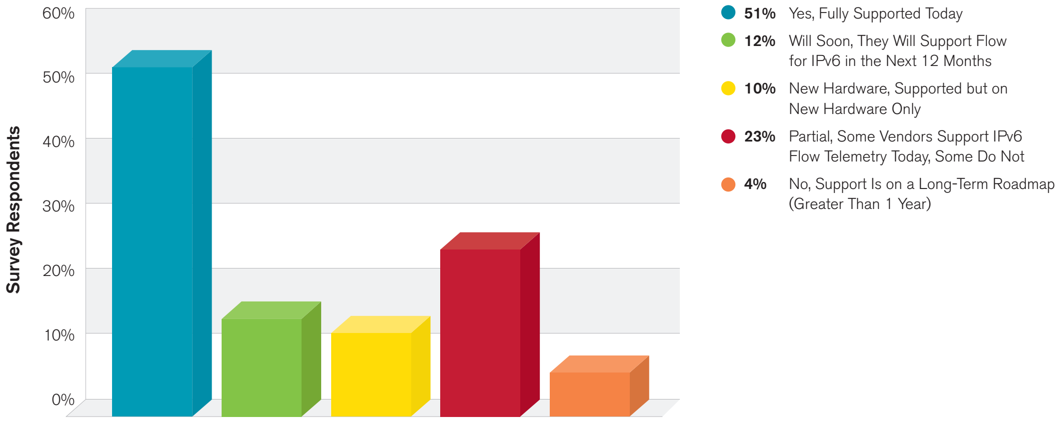


Figure 38 *Source: Arbor Networks, Inc.*

Just over half of respondents indicated that they use IPv6 on their management networks. In terms of providing IPv6 addresses to customers, more respondents offer IPv6 services to their business customers (Figure 39) as compared to their consumer customers (Figure 40).

IPv6 Addresses for Business Customers

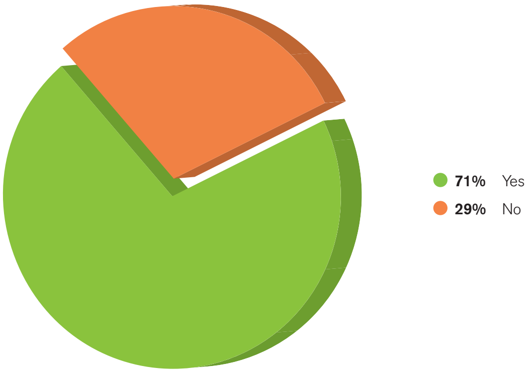


Figure 39 *Source: Arbor Networks, Inc.*

IPv6 Addresses for Consumer Customers

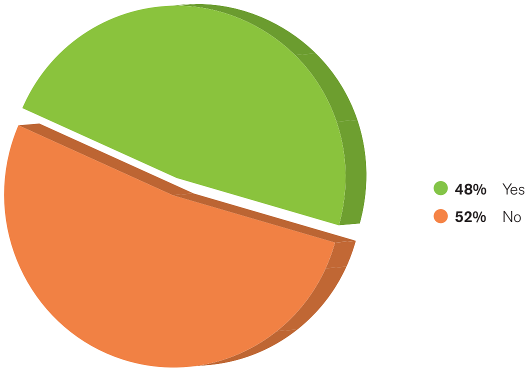


Figure 40 *Source: Arbor Networks, Inc.*

This year, the survey asked respondents for the peak daily rate of IPv6 traffic on their network. The highest reported traffic rate was 3 Gbps, with numerous responses at the sub-100 Mbps level. Although IPv6 traffic is growing relatively quickly in percentage growth terms, the actual volume of traffic is still very low compared to IPv4 (see *"ATLAS IPv6 Growth,"* page 39). The low adoption of IPv6 by consumers is a likely cause, especially given the increased availability of IPv6 services post-World IPv6 Launch. The slow adoption may be related to the lack of support for IPv6 and many widely deployed CPE devices.

When considering projected IPv6 traffic growth, 42 percent of respondents anticipate a 20 percent rise over the next 12 months, with 25 percent seeing more than 100 percent growth (Figure 41). Given the growth exhibited within ATLAS data, and the relatively low starting point in terms of actual traffic volumes, we believe that a higher percentage is likely. Some regions and countries, such as India, have already exhausted their available IPv4 address space. However, the responses illustrate that our respondents expect the growth of IPv6 traffic to remain slow.

IPv6 Traffic Growth

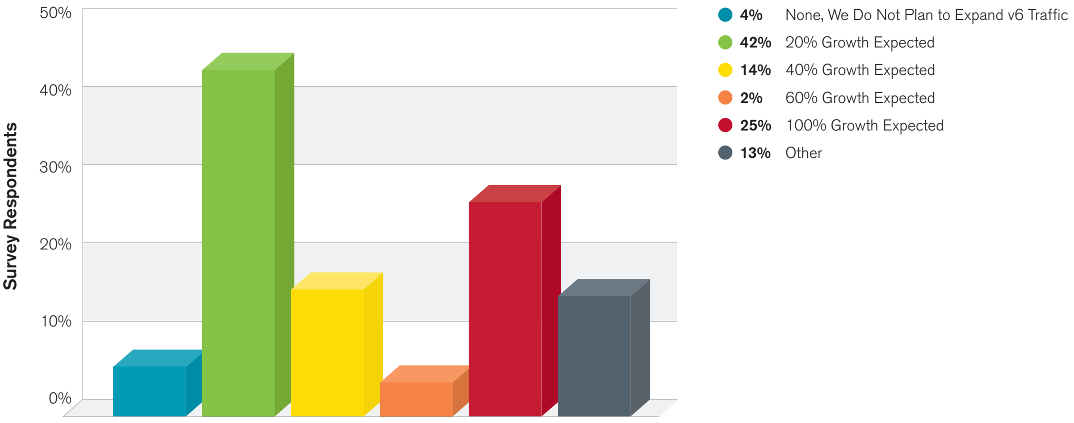


Figure 41 *Source: Arbor Networks, Inc.*

The IPv6 security concerns of respondents have shifted somewhat from last year's results (Figure 42). This year the top perceived threat is traffic floods or other DDoS attacks, with 70 percent of respondents showing a concern—up from 52 percent last year. This may indicate that respondents are taking a more active interest in the monitoring and protection of the availability of IPv6 services.

IPv6 Security Concerns

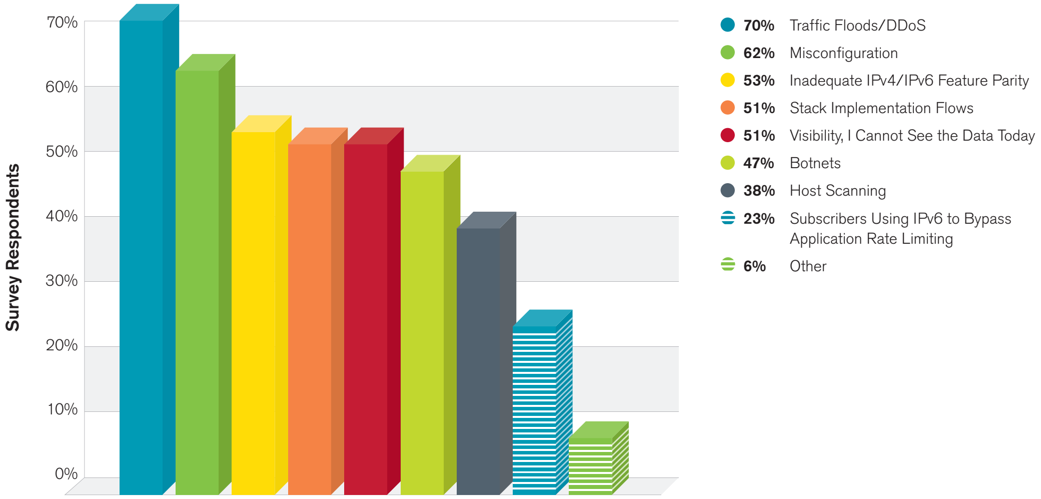


Figure 42 *Source: Arbor Networks, Inc.*

Last year the top concern—with 65 percent—was inadequate IPv6/IPv4 feature parity. This year only 53 percent were concerned in this regard. This could indicate that infrastructure vendors are now delivering more IPv6/IPv4 feature parity in their products.

Misconfiguration is still an IPv6 security concern for our survey respondents, with approximately 60 percent citing this issue over the last two years. The longer addressing and (relative) unfamiliarity with IPv6 may be a contributing factor. Last year's number two concern—lack of visibility—has dropped back from 60 percent to 51 percent. This reduction may be due to the increased proportion of respondents who have flow telemetry and/or visibility of IPv6 traffic, rather than a reduction in the importance of visibility overall.

ACLs remain the most popular attack mitigation technique for IPv6, despite their operational and functional limitations (Figure 43). The strong growth in the proportion of respondents planning to use IDMS to mitigate IPv6 attacks has continued this year—a nearly 13 percent rise from last year, where there had been an 11 percent rise from the year before. This may indicate that operators are looking to protect the availability of IPv6 services, or it may be due to increased IPv6 support within IDMS solutions.

One key change of note is that the percentage of respondents who do not intend to mitigate attacks against IPv6 services has fallen drastically from 20 percent to 8 percent. This is a clear indicator that IPv6 services are becoming more important to Internet operators.

IPv6 Mitigation Capabilities

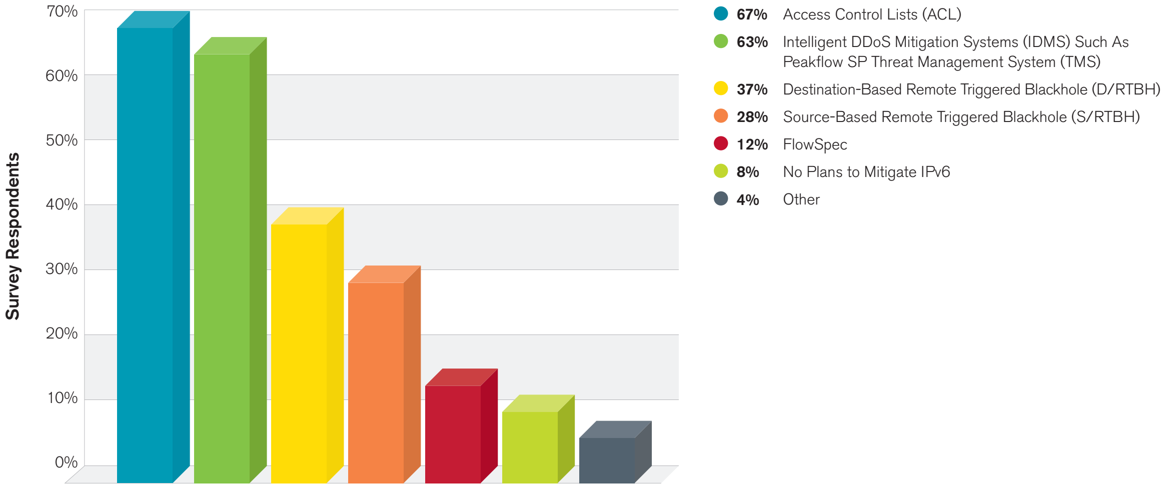


***Figure 43** Source: Arbor Networks, Inc.*

ATLAS IPv6 Growth

One of the traffic statistics gathered by ATLAS is the amount of native IPv6 traffic crossing the boundaries of participant networks, along with the growth of that traffic over time (Figure 44).

ATLAS IPv6 Traffic Growth

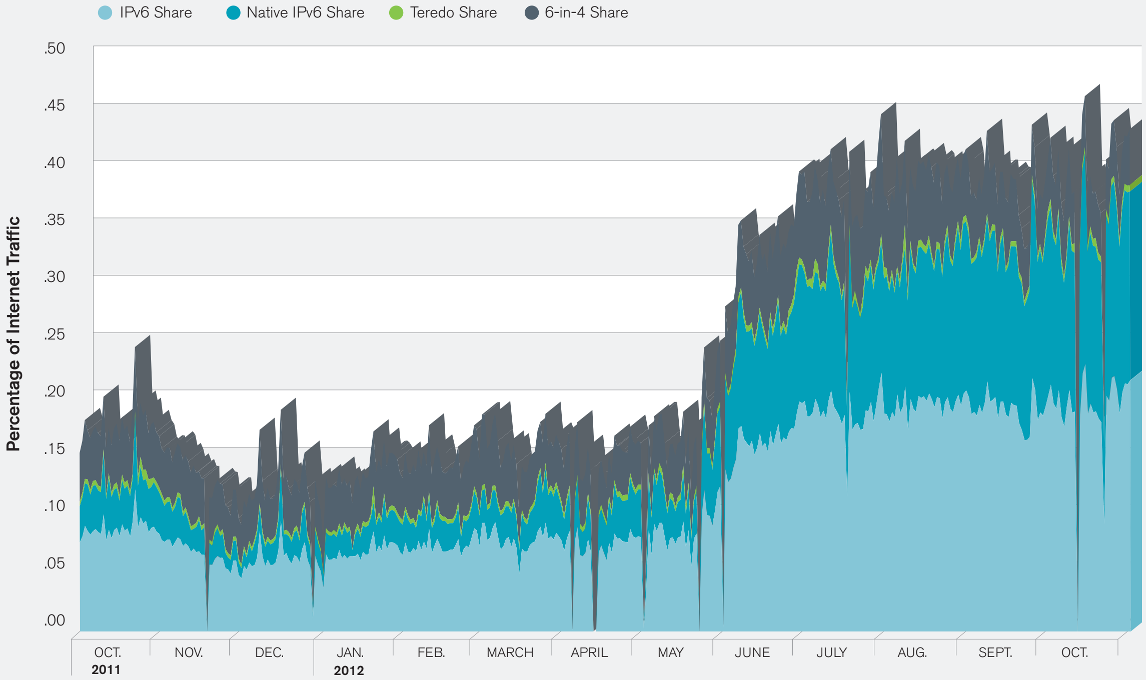


***Figure 44** Source: Arbor Networks, Inc.*

The peak, cumulative native IPv6 traffic volume monitored by ATLAS across approximately 250 participating network operators during the month of October 2012 was around 40 Gbps. This sounds like a lot, but the peak monitored volume of IPv4 traffic was 40.37Tbps—a big difference. However, we should consider that not all ATLAS respondents have the capability of monitoring native IPv6 traffic due to their configuration or network infrastructure.

Continued on page 40

ATLAS IPv6 Growth (continued)

In fact, at time of writing, fewer than 20 percent of ATLAS participants actually provide statistics on native IPv6 traffic. The geographic distribution of these respondents can be seen in Figure 45. Looking at those participants, native IPv6 traffic is, on average, responsible for 0.093 percent of their total Internet traffic. This is lower than the percentage reported earlier this year by the ATLAS system during coverage of World IPv6 Launch. This difference is due to the fact that additional ATLAS participants have now started providing native IPv6 statistics.

ATLAS IPv6 Native Traffic Reported by Region

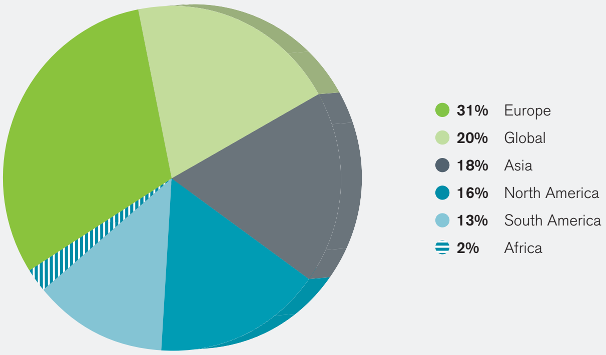


Figure 45 *Source: Arbor Networks, Inc.*

If we look at data from just the ATLAS participants who provided IPv6 statistics in the run up to World IPv6 Launch, then we see a gradual increase of IPv6 traffic on the Internet in the weeks before the day itself. This ramp-up resulted in IPv6 traffic growing from 0.06 percent to almost 0.15 percent of all Internet traffic on these networks, as previously reported. This growth appears to have continued. You can see from Figure 44, looking just at this set of ATLAS participants, IPv6 traffic stood at around 0.22 percent of Internet traffic at the end of October 2012.

Corporate Network Threats (Non-Enterprise)

This year an additional section has been included in the survey to ascertain the security concerns, monitoring techniques and policies used by non-enterprise respondents on their internal networks. These networks, incorporating both corporate and C&C functions, are important to network operators to ensure that their business, service provider networks and customer services are managed and controlled effectively.

The top two security threats experienced by respondents on their internal networks during the survey period are "botted compromised hosts" and "under-capacity for Internet bandwidth (due to DDoS or other event)," with nearly half of respondents reporting each of these issues (Figure 46). The increase in botted hosts is not surprising given the number and complexity of malware variants that exist, their rate of evolution and the consequent inability of IDS and AV systems to fully protect us.

Nearly 20 percent of respondents reported experiencing either a malicious insider or APT on their internal network during the survey period. These types of threats can be difficult to detect as they occur inside the security perimeter and are designed to be stealthy. Solutions aimed at detecting and mitigating these kinds of threats are a recent focus for the information security industry, and given these results, this focus is justified.

Internal Network Security Threats

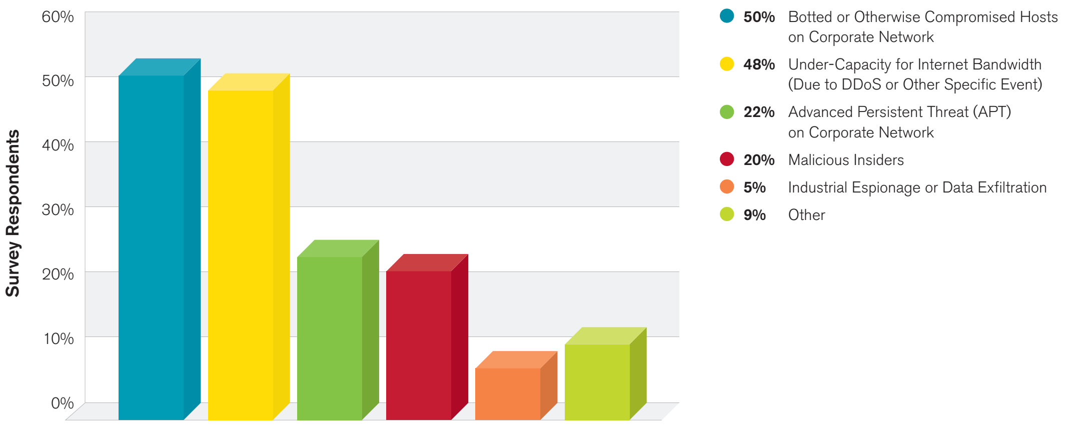


Figure 46 *Source: Arbor Networks, Inc.*

Botted hosts continue to be the top security concern for internal networks over the upcoming year (Figure 47). However, there is a lot more concern moving forward about APT, industrial espionage, data exfiltration and malicious insiders. The mainstream press coverage around Flame, various data thefts, the Saudi Aramco Shamoon incident and other events likely contributed to this.

Internal Network Security Concerns

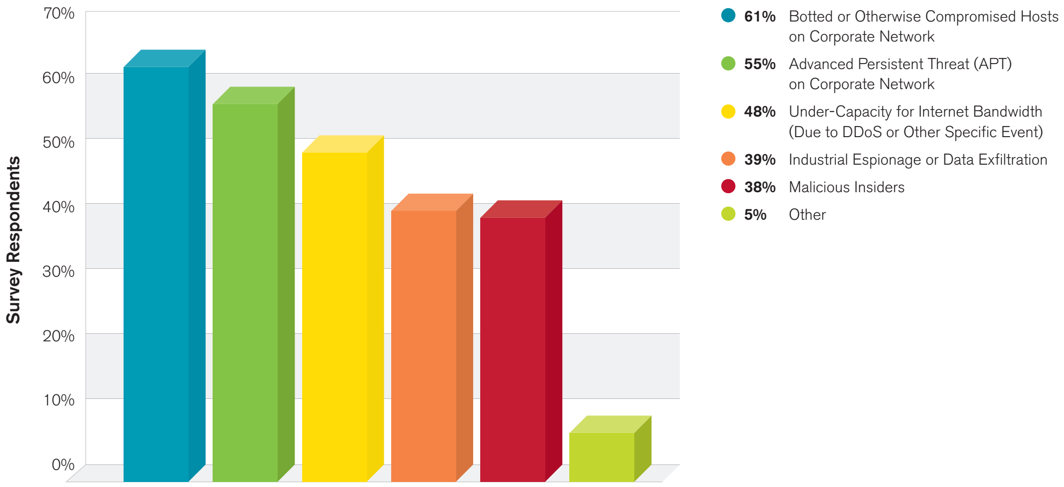


Figure 47 *Source: Arbor Networks, Inc.*

This year the survey asked respondents about their policies in relation to social media and BYOD on their internal networks. Unsurprisingly, nearly three-quarters of respondents allow the use of social media sites from work, with half of respondents also allowing instant messaging applications to be used. In fact, only 13 percent actively block access to these applications and sites.

Sixty-three percent of respondents allow employees to utilize their own devices on the corporate network (Figure 48). This illustrates that many organizations are trying to leverage the reduced costs and increased productivity that BYOD can bring. However, when it comes to allowing these devices to access cloud services for synchronization, more than half of respondents do not allow this (Figure 49). This indicates that our respondents are sensitive to where their business data and intellectual property may reside.

Use of BYOD

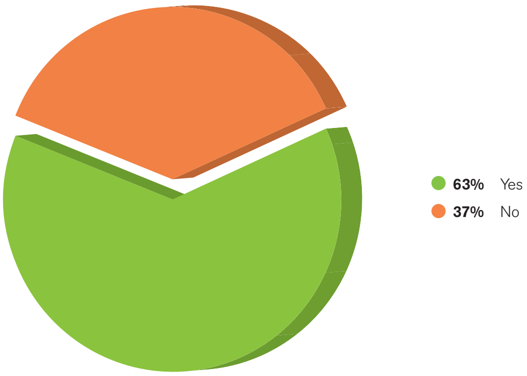


Figure 48 *Source: Arbor Networks, Inc.*

Use of Cloud Device Synchronization Services

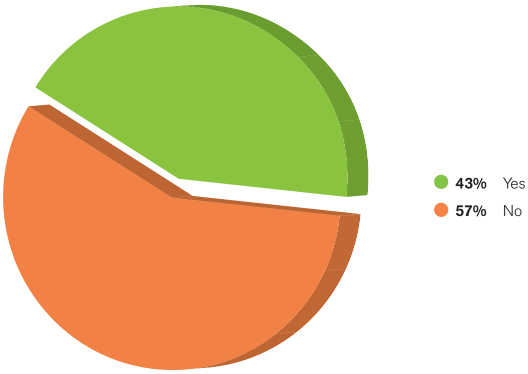


Figure 49 *Source: Arbor Networks, Inc.*

A cause for concern is that more than half of respondents have no solution in place to actually monitor or detect employee-owned devices on their networks. This is a potential security issue given the volumes of data many devices are capable of copying/storing, and growing concerns around malicious insiders, APT and data exfiltration.

Looking more broadly at threat detection, a wide range of mechanisms are used to detect threats on the internal network, with firewall and IDS being by far the most commonly used detection method (Figure 50). Around half of respondents also use commercial IP flow processing tools and/or in-house developed scripts and tools to monitor their internal networks.

Internal Network Threat Detection Mechanisms

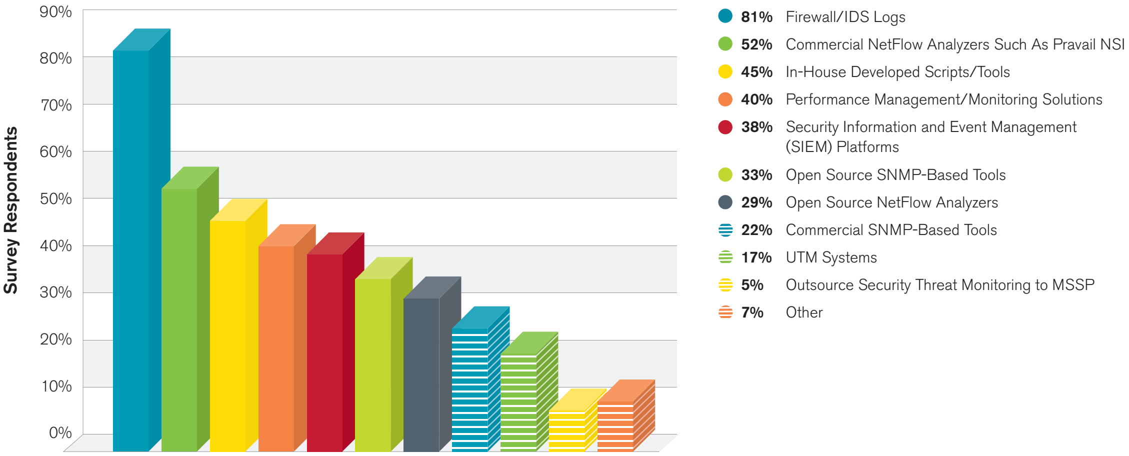


Figure 50 *Source: Arbor Networks, Inc.*

Data Centers

Data centers are increasingly being targeted by attacks with 94 percent of data centers seeing DDoS attacks regularly. Data center customers are the most common attack targets.

With the current trends toward cloud computing and data center consolidation, it is important to keep up with developments relating to traffic analysis techniques, DDoS attacks, DDoS mitigation and other points of interest regarding data centers. Approximately 63 percent of survey respondents offer data center services to their end customers, an identical percentage to last year.

When asked how much visibility data center operators have into their networks, just over three-quarters of respondents indicated that they have good visibility up to Layer 4, while a third indicated that they have visibility up to Layer 7 (Figure 51). This indicates that the majority of operators are likely blind to attacks above Layer 4, making it difficult to effectively defend against them. Layer 7 DDoS attacks are especially dangerous as they are typically "low and slow," and are often undetectable using traditional volumetric detection mechanisms.

Visibility into Data Center Networks

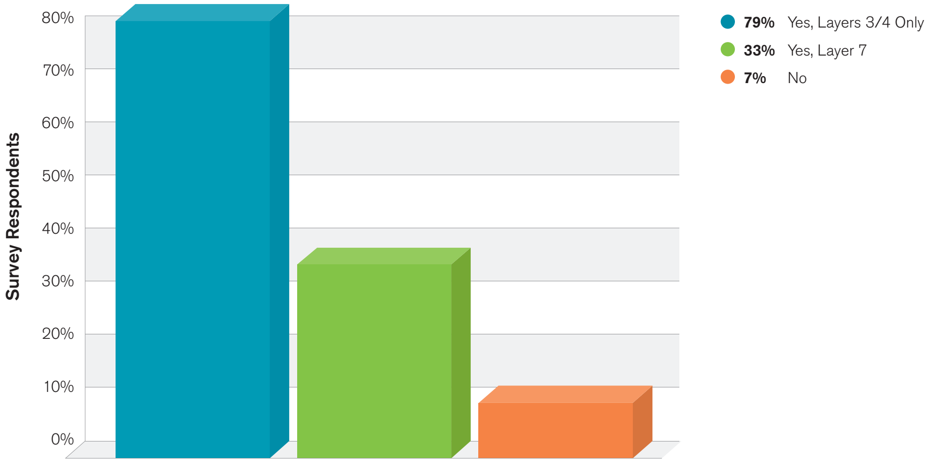


Figure 51 *Source: Arbor Networks, Inc.*

In terms of deployed security devices, firewalls are standard practice in data centers, as one would expect (Figure 52). The second most commonly deployed technology is IDS/IPS, with slightly more than half of respondents employing this technology. Interestingly, this data differs substantially from last year's survey, where only 42 percent of respondents had firewalls deployed.

Data Center Security Techniques

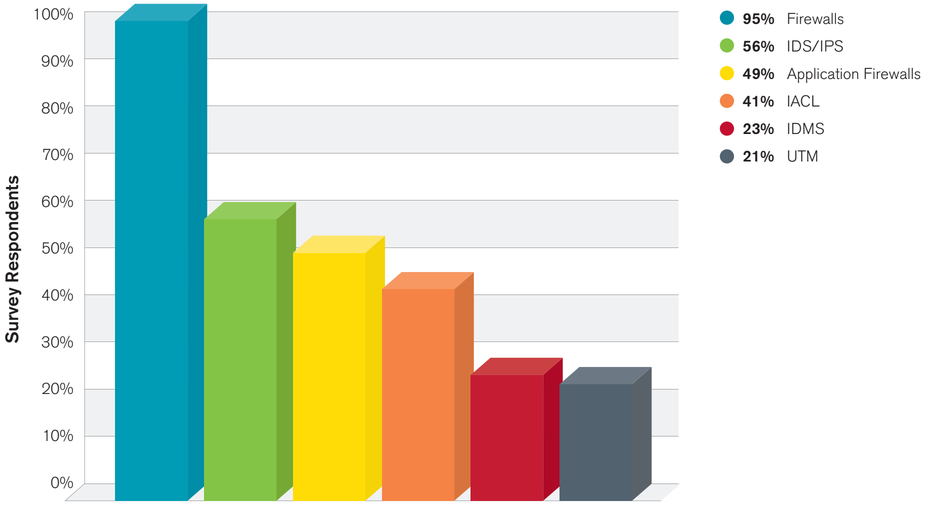


Figure 52 Source: Arbor Networks, Inc.

It is worth noting that just over one-third of respondents indicated that their firewalls or IDS/IPS systems were compromised by a DDoS attack during the survey period (Figure 53). However, last year 42 percent experienced this issue, so there has been some improvement here. This improvement may be a result of operators putting in measures to specifically shield their firewall and IPS from attacks.

Firewalls or IDS/IPS Compromised by DDoS Attack

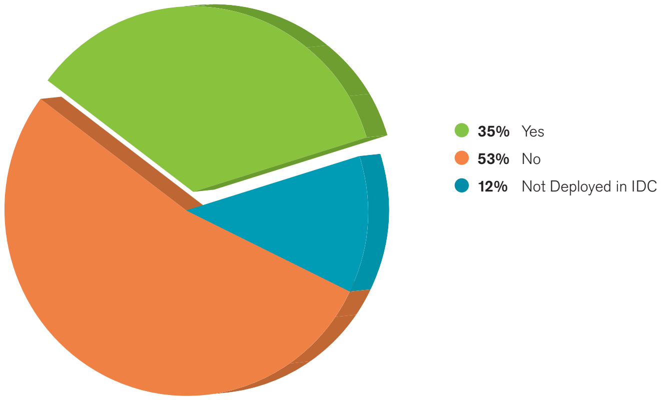


Figure 53 Source: Arbor Networks, Inc.

Data centers inherently contain numerous targets for DDoS attacks. Over 45 percent of respondents have experienced a DDoS attack against their data center during the survey period. This is a drop from 56 percent last year.

Of the respondents who did suffer a DDoS attack, nearly 17 percent reported that the volume of the attack exceeded the available bandwidth into their data center. This is a decrease from the last survey, where 25 percent of respondents reported that attacks had exceeded their available bandwidth. This decrease is likely due to increased utilization of application-layer attack vectors, increased deployed capacity and the use of DDoS mitigation technologies by upstream bandwidth providers.

Data center operators report that the most frequent target of DDoS attacks is their customers (Figure 54). Data center infrastructure services (e.g., DNS, SMTP) are the second most frequent target with just over one-half of respondents experiencing these attacks, while one-third reported that the data center infrastructure itself was attacked.

Targets of DDoS Attacks in the Data Center

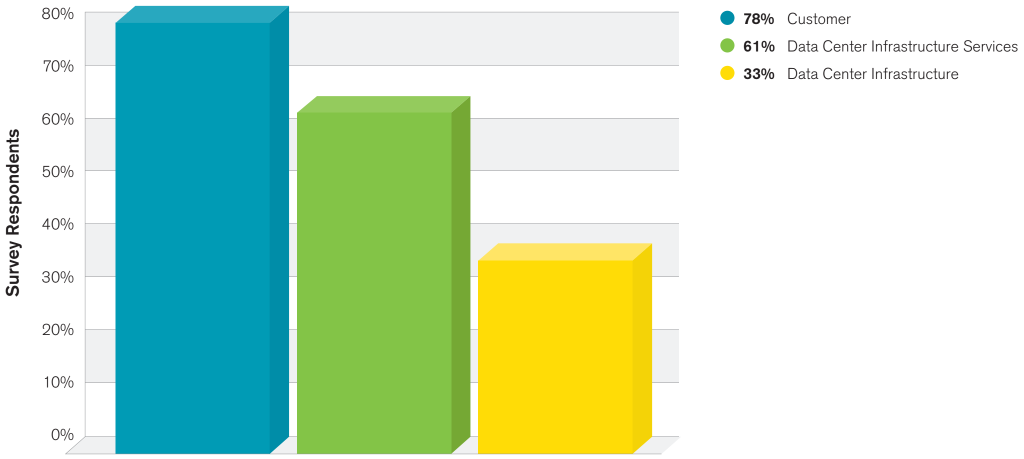


Figure 54 *Source: Arbor Networks, Inc.*

The proportion of respondents who saw attacks against data center customers declined slightly from 87 percent to 78 percent. However, there were significant increases in the proportion of respondents who saw attacks against both the data center infrastructure services and data center infrastructure itself since 2011. These proportions increased from 42 percent to 61 percent and 13 percent to 33 percent respectively. This may indicate that attackers are renewing their focus on data center infrastructure.

For data center operators who reported being the victims of a DDoS attack, the observed frequency of the attacks increased over last year's survey, as expected (Figure 55). In 2011, 30 percent of respondents indicated that DDoS attacks were not a monthly occurrence; this has since declined to just under 6 percent. In fact, 83 percent of respondents who were victims of attack now experience between one and 50 attacks per month.

Frequency of Attacks (Per Month)

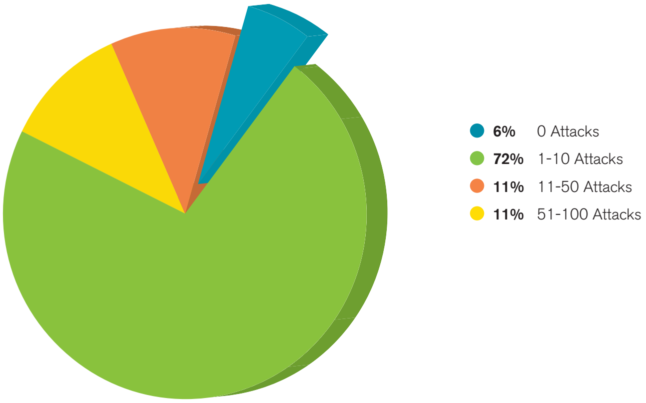


Figure 55 *Source: Arbor Networks, Inc.*

Nearly 90 percent of data center operators reported operational expenses as a business impact due to DDoS attacks (Figure 56). This should come as no surprise since bandwidth comes at a cost, failure to meet SLAs can result in hefty penalties and attacks can be time-consuming to deal with—wasting valuable resources.

Business Impact of Attacks

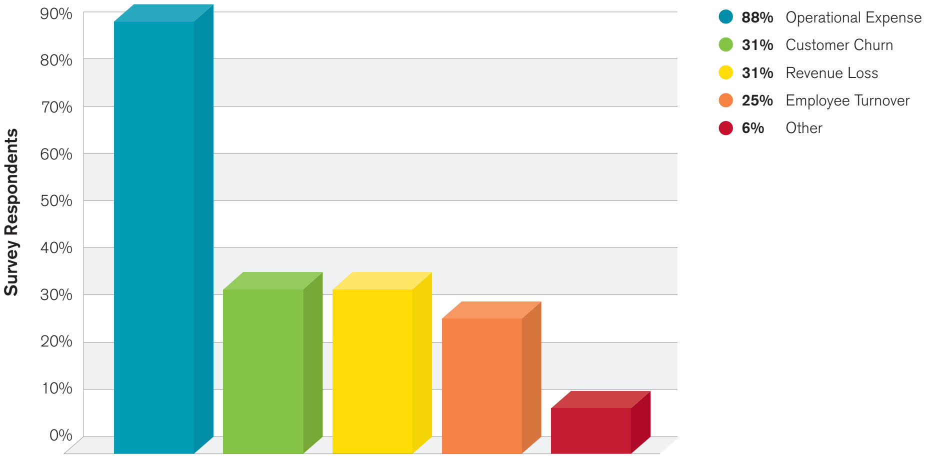


Figure 56 *Source: Arbor Networks, Inc.*

Customer churn was reported by approximately one-third of operators. Again, this is quite understandable, as customer confidence in the availability of data center services can be shaken should the services become unavailable. Customers may then feel that it is better to switch to a data center that has better protection from DDoS attacks.

Finally, one-third of operators reported a business impact of revenue loss due to DDoS attacks, a similar percentage to last year. This may be because data center customers are not required to pay for their services when they are unavailable, or because the primary business of the organization is affected by an attack.

Firewalls and IPS devices can be negatively impacted by DDoS attacks due to state exhaustion, as mentioned earlier. Similar to firewalls and IPS devices, load balancers also maintain state and may be adversely impacted by a DDoS attack. More than 29 percent of respondents indicated that their load balancer devices suffered when subjected to a DDoS attack (Figure 57). This is a decline from 2011, where 43 percent of respondents indicated that their load balancers were impacted. This is a positive trend and may be a result of operators having put measures in place to shield these stateful devices from attack.

Load Balancers Compromised by DDoS Attacks

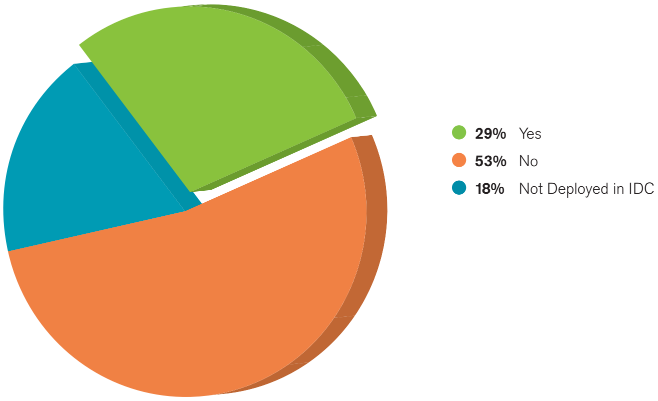


Figure 57 *Source: Arbor Networks, Inc.*

Data center operators use a wide variety of DDoS prevention/mitigation techniques. In general, the proportion of respondents using the various techniques remained unchanged from last year's survey (Figure 58). However, there was a 10 percent increase in the proportion of respondents using IDMS and an approximate 22 percent decrease in the proportion using D-RTBH. This may indicate that data center operators are becoming more focused on protecting end-customer service availability during an attack. Interestingly, almost three-quarters of data center operators who have IDMS solutions deployed offer their customer base an anti-DDoS service based on their own IDMS equipment, thus monetizing their investment.

DDoS Protection Techniques in the Data Center

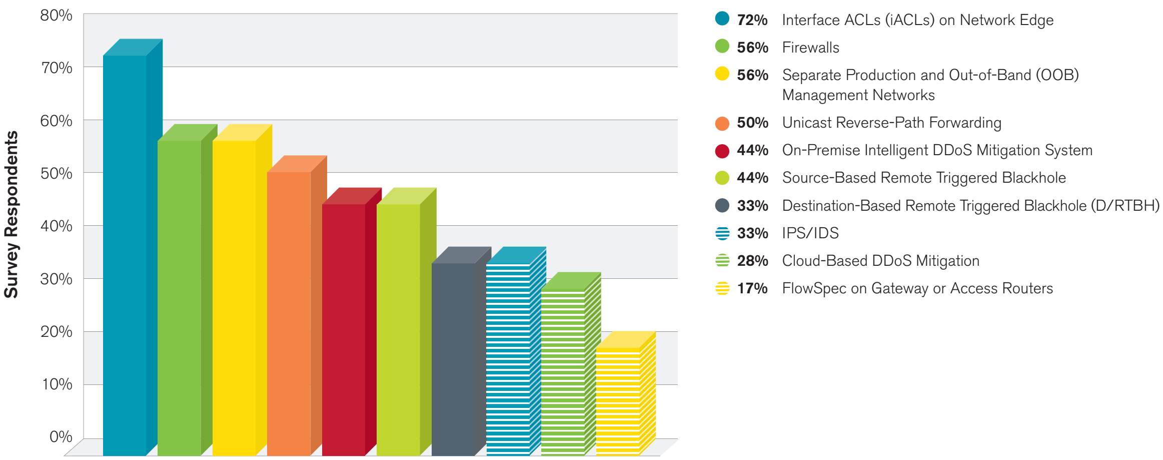


Figure 58 *Source: Arbor Networks, Inc.*

Most concerning, though, is the significant increase in the proportion of data center operators who are using firewalls and IDS/IPS devices to deal with DDoS attacks. There are significant risks involved in relying on firewalls and IPS for DDoS protection. Although these devices can deal with some kinds of DDoS attacks, they are primarily designed to assure confidentiality and integrity, rather than service availability.

Lastly, half of the survey respondents indicated that they monitor either intra data center traffic or outbound traffic for signs of compromised devices. This is a decline from 2011, where more than 57 percent of respondents indicated that they monitor such traffic. This decrease is a concern as we have seen attacks launched from within data centers this year. Specifically, the Operation Ababil attacks against American financial institutions in late 2012 used compromised servers to launch DDoS attacks. These attacks were particularly severe because they leveraged the bandwidth and processing capacity that these servers possess.

Mobile/Wireless Networks

The roll-out of LTE services has accelerated increasing the bandwidth available to mobile subscribers. But, operators still have visibility limitations and a reactive stance on subscriber security.

With the increased worldwide adoption of and dependence on wireless networks, it is no surprise that 32 percent of survey respondents operate wireless networks, up from 25 percent last year. The number of subscribers on respondent networks is impressive and underscores the importance of the availability of these networks (Figure 59). Wireless infrastructure has long ago transitioned from being a luxury to a necessity. In fact, two-thirds of respondents have more than one million subscribers and nearly one-quarter report networks with more than 25 million subscribers.

Subscriber Base on Wireless Networks

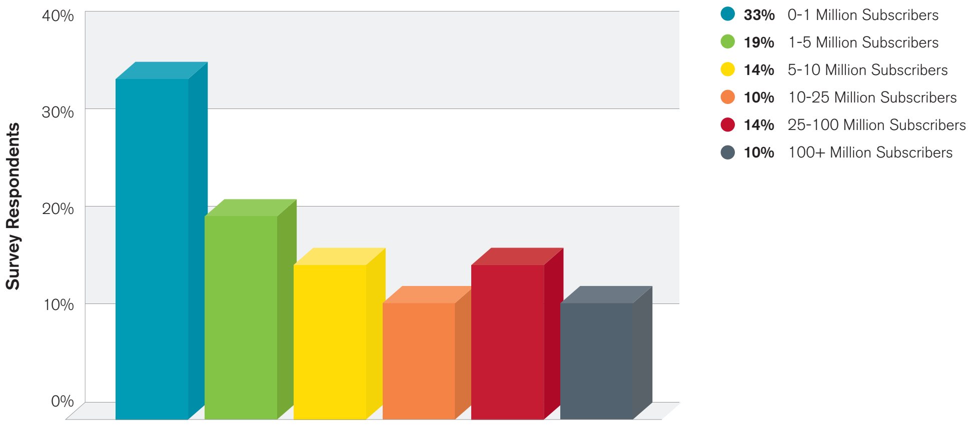


Figure 59 *Source: Arbor Networks, Inc.*

As expected, most respondents operate traditional GSM 2G and 3G networks. However, LTE deployments continue to increase, with 53 percent of operators indicating that they have LTE deployed, versus nearly 29 percent in 2011 and approximately 10 percent in 2010 (Figure 60). WiMax deployments also increased, but only from approximately 5 percent in 2011 to nearly 6 percent in 2012, indicating that this is still a niche technology.

Deployed Wireless Technologies

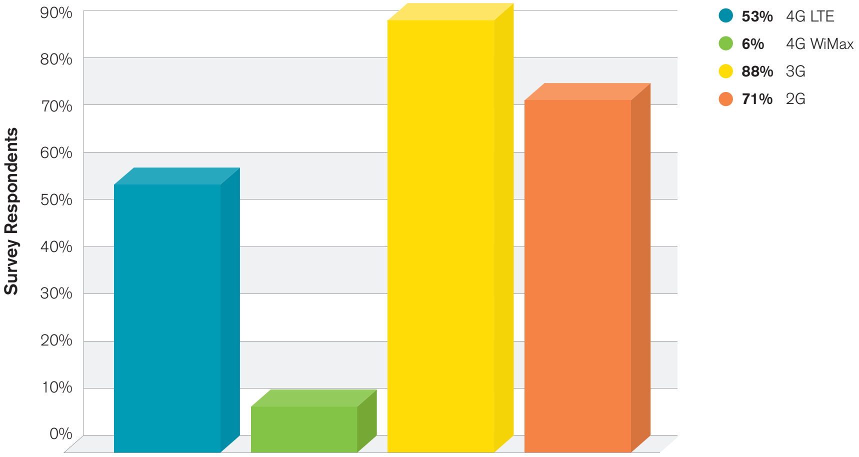


Figure 60 *Source: Arbor Networks, Inc.*

The percentage of operators already offering 4G services increased to approximately one-third from 19 percent in 2011, indicating continued strong adoption (Figure 61). This strong adoption rate becomes even clearer when we see that 45 percent of the remaining respondents plan to deploy LTE in the next two years, leaving only 22 percent with no current plans for adoption.

Commercial Availability of 4G

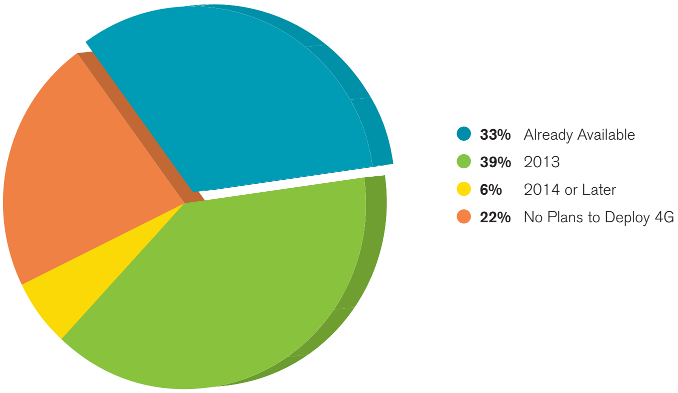


Figure 61 *Source: Arbor Networks, Inc.*

The use of NAT on wireless networks for subscribers is relatively common, with more than 72 percent of respondents indicating that they have NAT in place, up 10 percent over last year. This can protect operators from the ongoing shortage of IPv4 address space, and subscribers from unsolicited traffic and attacks. However, NAT devices pose a potential availability risk when subjected to DDoS attacks due to their stateful nature.

In the 2011 survey, over 59 percent of operators stated that they were using, or had plans to use, IPv6 technology in their networks—indicating a decline in the anticipated use of IPv6 in these networks. This may indicate a willingness to continue to use NAT as a solution for addressing within mobile networks well into the future.

Nearly 18 percent of respondents are now using IPv6 either for subscriber or mobile infrastructure addressing, a 50 percent increase over last year (Figure 62). Thirty percent of operators indicated that they are currently using, or plan to use, IPv6 over the next 12 months.

Use of IPv6 Addressing for Subscriber Devices and Mobile Infrastructure

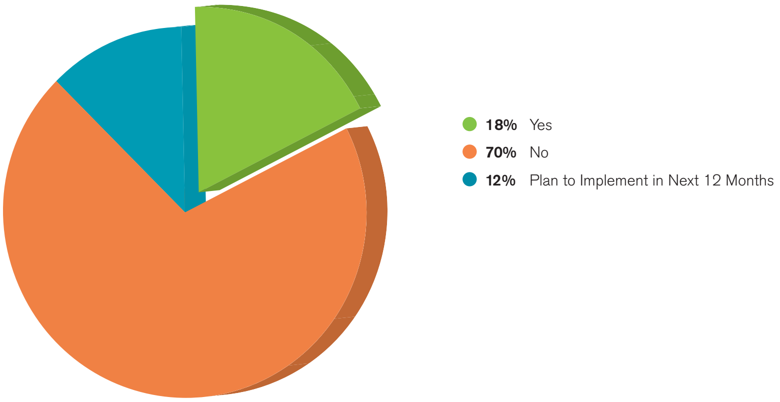


Figure 62 *Source: Arbor Networks, Inc.*

This year, more than one-third of respondents indicated that they have suffered a customer-visible outage due to a security incident, up from just over 12 percent last year. This is a significant increase and indicates the need for greater focus on security from mobile operators.

However, over 57 percent of respondents do not know what proportion of subscriber devices on their networks are compromised and are participating in botnets or other malicious activities. This is indicative of poor visibility in this regard. Many mobile devices are now as powerful as some laptop computers, with dual-core CPUs, gigabytes of memory and high-speed wireless interfaces. The malware problem in the mobile space is quite real, and large-scale malware activity—with thousands of active participants—could have a devastating impact on the resources of a wireless infrastructure.

Misbehaving user applications can also pose a real problem for mobile operators (Figure 63). A widely deployed misbehaving user application can present a significant availability threat, similar in some ways to a DDoS attack. Anecdotally, multiple operators have reported significant outages or performance issues caused by non-malicious but misbehaving user applications.

The majority of operators who suffered incidents relating to poorly behaving applications took a reactionary stance toward detection and mitigation, with over 30 percent indicating that they had to perform a reactive analysis of the problem. This is an unfortunate statistic, but is a direct result of the consumer broadband-based business model that mobile providers work within. Each subscriber contributes a relatively small amount of revenue to the provider, and every time the subscriber calls into the provider help desk, that revenue is offset for some time by cost. There is little incentive to put measures in place that could result in that subscriber calling in less often; hence, the more reactive approach. This model is likely to change if/when attacks impact the mobile network itself.

Detection of Poorly Implemented Mobile User Applications

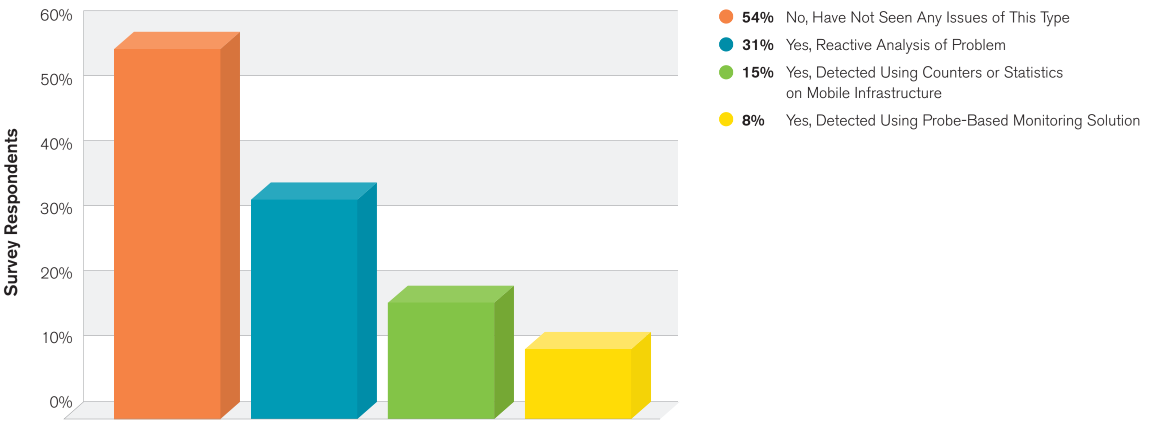


Figure 63 *Source: Arbor Networks, Inc.*

Unsurprisingly, given the above, a full 60 percent of respondents do not have visibility into the traffic on their mobile/evolved packet cores (Figure 64). One-third have visibility into the user/data-plane traffic, while approximately 27 percent have visibility into the control-plane traffic. The risk to the large percentage of operators who have no visibility into traffic on their packet core is clear: unseen threats cannot be prevented or contained.

Visibility of Traffic on Mobile/Evolved Packet Core

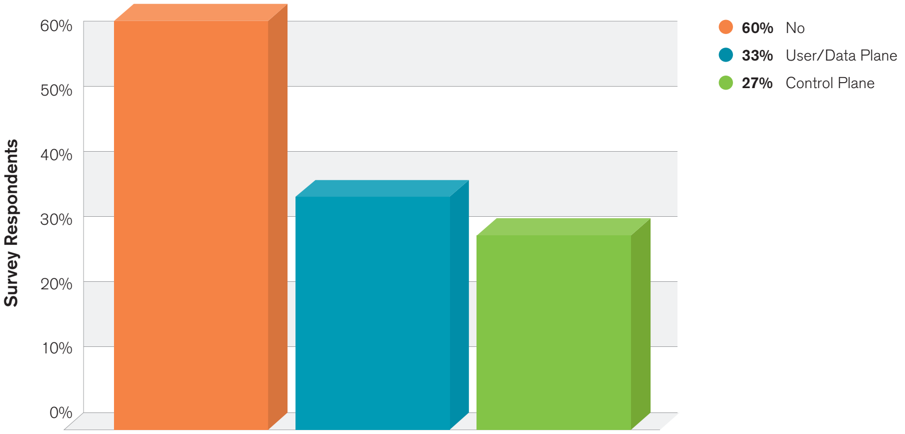


***Figure 64** Source: Arbor Networks, Inc.*

Of those respondents who have visibility into traffic on their mobile packet core, the majority use counters and statistics available directly from the mobile infrastructure itself, while slightly more than one-third of operators use vendor-supplied probe-based monitoring solutions (Figure 65).

Methods of Visualizing Traffic on Mobile/Evolved Packet Core

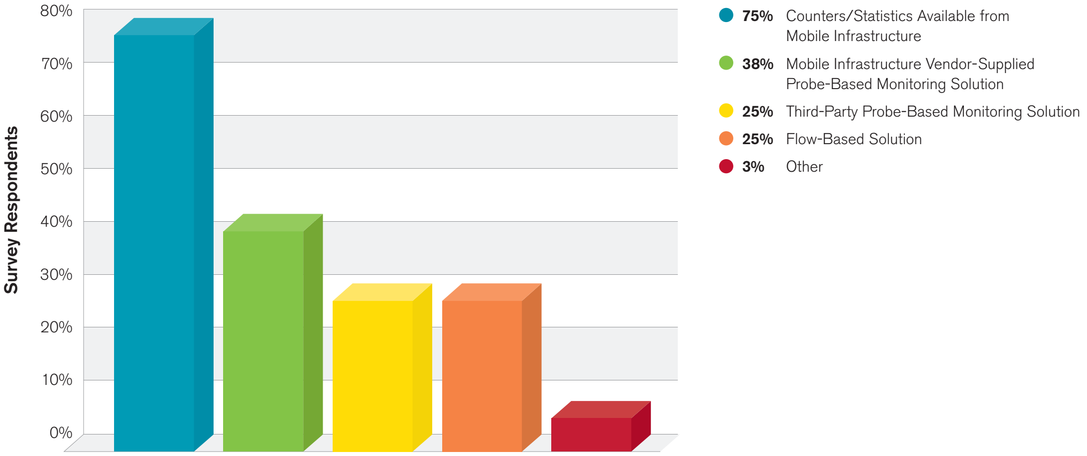


***Figure 65** Source: Arbor Networks, Inc.*

The remainder use third-party probes or a flow-monitoring device (such as Peakflow® SP) to visualize traffic. The low use of flow for network monitoring in this area may in part be due to the fact that packet core traffic may be tunneled, making Layer 3/4 information derived from the outer IP header less useful.

Mobile operators utilize a wide variety of tools and techniques to protect their infrastructures against availability threats (Figure 66). This year, there was a 19 percent increase in the use of IDMS, up from 37 percent to 44 percent. There was a corresponding decrease in the proportion of respondents using the security features in their data and signaling gateways, down from 42 percent last year to almost 19 percent. iACLs and NAT/PAT technology are the most common protective measures, despite their limitations.

Security Measures to Protect Services Against Availability Threats

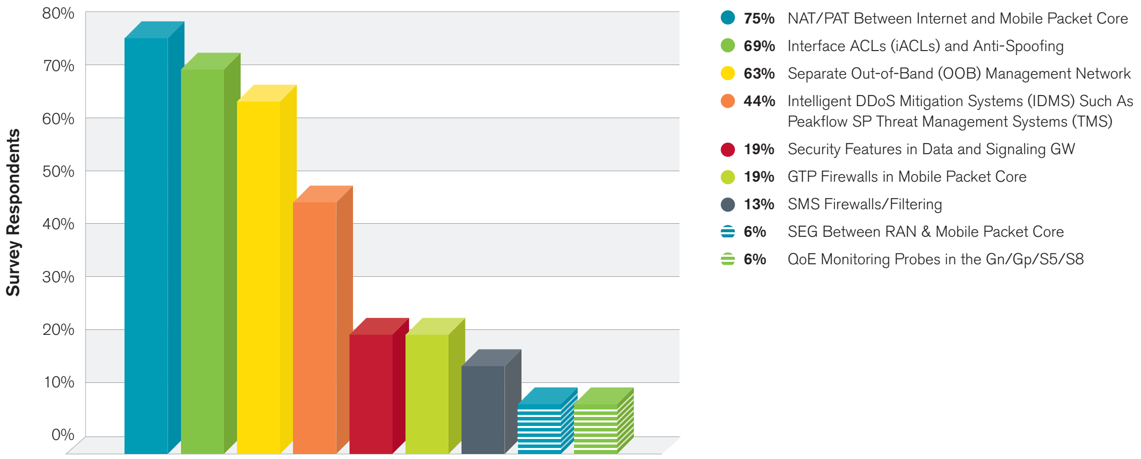


Figure 66 *Source: Arbor Networks, Inc.*

Approximately 28 percent of respondents have seen DDoS attacks targeting their mobile users, RAN, back-haul or packet core—a small increase over last year—while nearly half of respondents have not seen any attacks (Figure 67). Roughly one-quarter don't know if these attacks are occurring due to a lack of visibility. For those seeing attacks, attack frequency was consistent from all respondents at between one and 10 events per month.

In terms of the targets of these attacks, firewalls and user handsets are the most commonly affected devices.

Inbound DDoS Attacks Targeted Toward Wireless Networks

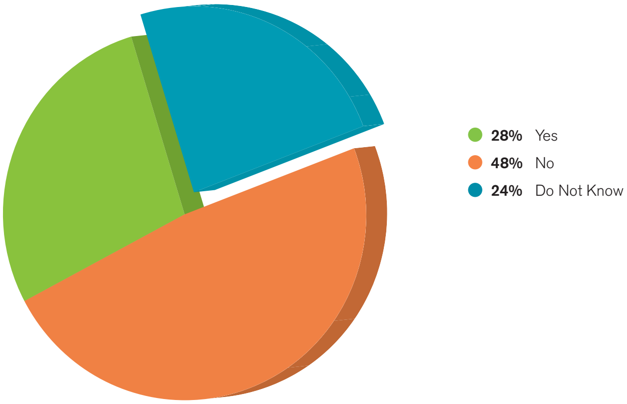


Figure 67 Source: Arbor Networks, Inc.

Looking at mobile Internet (Gi) infrastructure, nearly two-thirds indicated that they have visibility into traffic at Layers 3 and 4, with more than 29 percent having Layer 7 visibility (Figure 68).

Visibility on Mobile Internet (Gi) Backbone

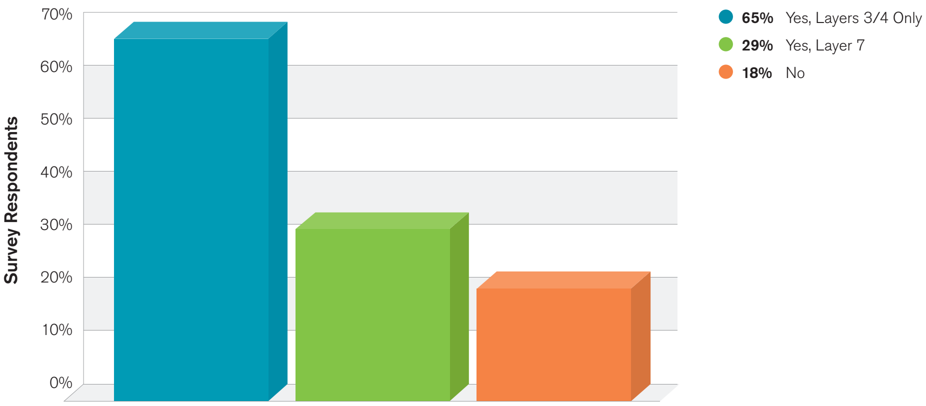


Figure 68 Source: Arbor Networks, Inc.

A variety of solutions are used to gain visibility into traffic, with infrastructure counters and statistics being the most common mechanism (Figure 69). Flow is the second most common mechanism in this more traditional ISP-like environment.

Gi Traffic Visibility Solution

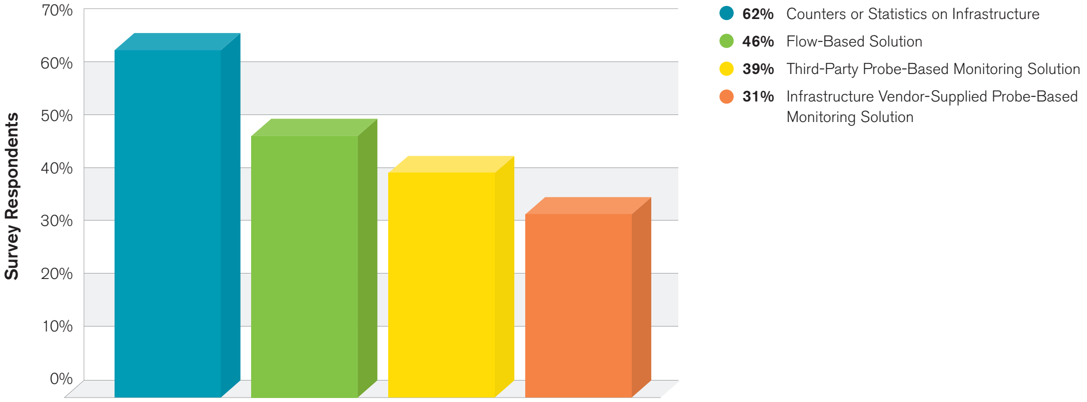


Figure 69 *Source: Arbor Networks, Inc.*

Although mobile malware is a reality, it would appear from these results that DDoS-capable mobile malware is still in its infancy, with only 16 percent of respondents indicating that they have seen outbound attack traffic from subscribers (Figure 70). However, more than one-quarter of respondents don't know whether their subscribers are originating DDoS traffic.

DDoS Attack Traffic Originating from Mobile Subscribers

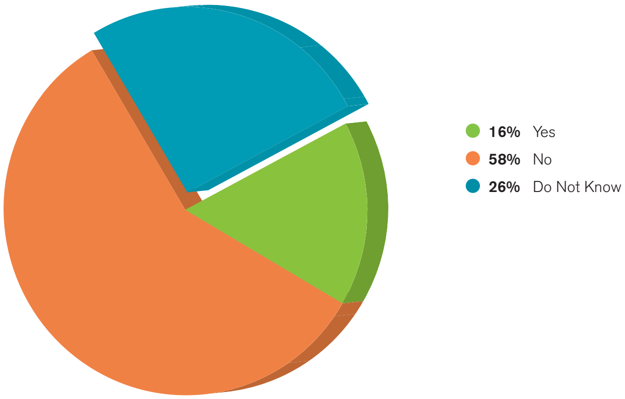


Figure 70 *Source: Arbor Networks, Inc.*

One fact remains, however: the number of mobile devices, along with the sophistication and power of these devices, continues to increase year over year. We believe it is only a matter of time before botnets and DDoS become more prevalent within mobile infrastructure.

In terms of mitigating outbound attacks from subscribers, only 17 percent of respondents indicated that this is something they would do, with nearly three-quarters having no plans in this regard (Figure 71).

Subscriber Outbound DDoS Mitigation

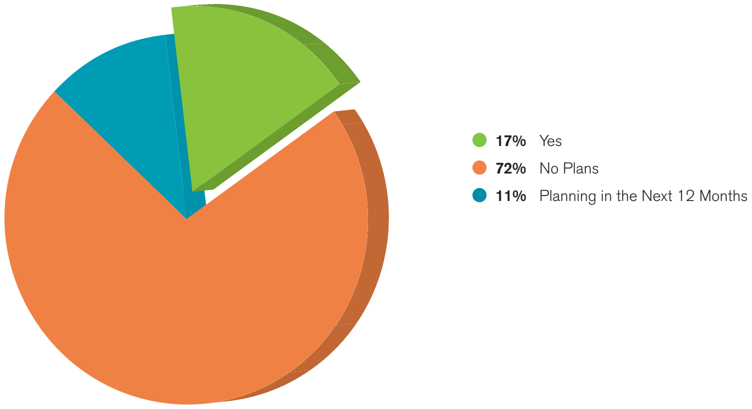


Figure 71 *Source: Arbor Networks, Inc.*

Only 10 percent of respondents indicated that they have seen DDoS attacks impacting their mobile Internet (Gi) infrastructure. This is a surprisingly low number given contrary anecdotal evidence in this regard. However, this may be partially explained by the fact that 45 percent of respondents simply don't know if they are being targeted or not—potentially demonstrating a lack of monitoring and threat detection capability (Figure 72).

DDoS Attack Impact on Internet (Gi) Infrastructure

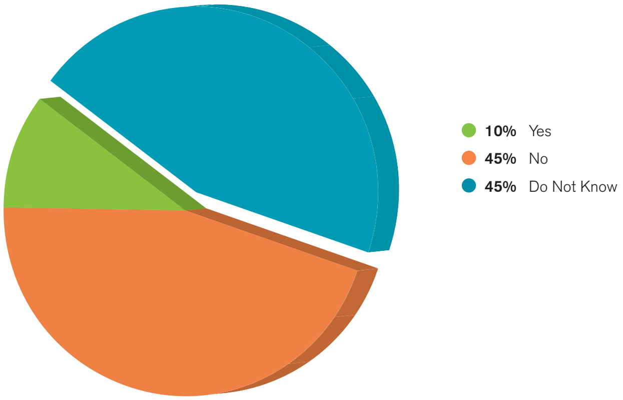


Figure 72 *Source: Arbor Networks, Inc.*

For those seeing attacks, half of respondents saw between one and 10 attacks per month, with the other half seeing between 11 and 20 attacks per month targeting their Gi infrastructure. Interestingly, the targets of these attacks were solely cited as being the DNS servers or router/links (congestion). No operators reported seeing attacks specifically targeting firewalls or NAT infrastructure. This is contrary to some information received outside of the survey from mobile operators during the past year.

Given the speed of evolution in mobile technologies and our increased dependence on mobile networks, mobile operators are having to upgrade their infrastructure to maintain competitiveness. At the same time, they should implement threat detection and monitoring solutions to protect themselves and their customers.

MSSP

Approximately two-thirds of respondents are offering managed DDoS solutions. Technologies used to implement the services are varied. MSSPs found that customers activate their DDoS mitigation services five times per year on average.

Over 61 percent of this year's respondents offer managed security services to their customers. Service provider respondents offer a variety of different managed services with managed router, managed firewall, and traffic visibility and reporting topping the list (Figure 73). Approximately two-thirds of respondents are offering managed DDoS solutions. This represents an increase in nearly every type of managed security service offering when compared to last year's results.

Managed Services Offered

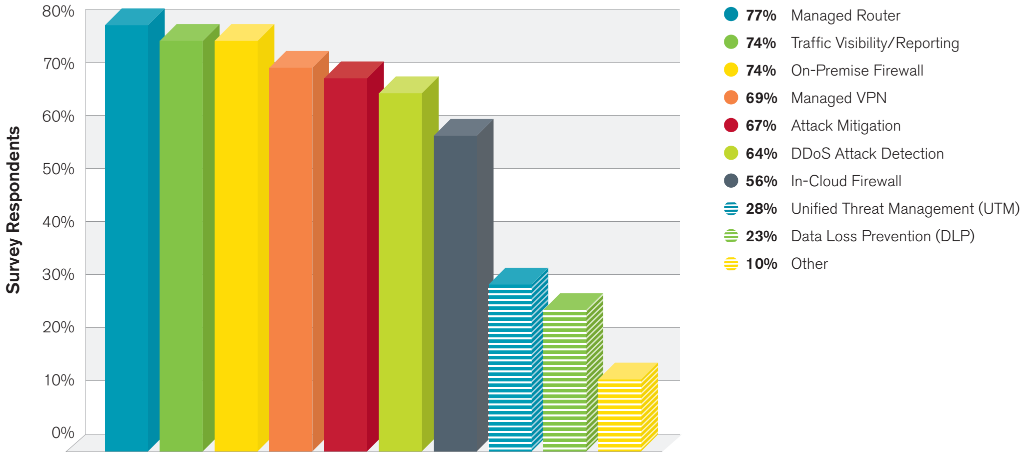


Figure 73 *Source: Arbor Networks, Inc.*

Looking more specifically at DDoS detection and mitigation services, respondents cited a number of criteria that their customers use for evaluating competitive DDoS protection services. The most common are:

- Price of the service compared to others
- Amount of mitigation capacity
- Mitigation activation time based on SLA
- Access to experienced SOC personnel

The majority of MSSPs provide tiers of DDoS protection services incorporating different reporting, mitigation and portal options. These are offered both as cloud-based services and managed network perimeter devices. Technologies used to implement the services are varied and include the following: IDMS, interface ACLs, source/destination-based remote black hole triggering, firewalls and IPS/IDS. The majority of MSSPs also reported offering a DDoS protection service portal so that customers can view their traffic levels, attacks and mitigations. In addition, SLAs for DDoS mitigation reaction time are fairly common but not universal among respondents. Lastly, MSSPs found that customers activate their DDoS mitigation services five times per year on average.

VoIP Operators

Nearly 80 percent of operators have the ability to detect threats against VoIP infrastructure. Operators leveraging commercial tools for visibility nearly doubled from last year's report, and the percentage with no visibility dropped by 25 percent from last year's survey. Half of the respondents saw incidents of toll fraud attacks against their VoIP networks.

Approximately 21 percent of operators indicated they have a dedicated VoIP security team. While over half utilize their main security group for VoIP, slightly more than one-quarter indicated they have no group responsible for VoIP security (Figure 74). These numbers all represent modest improvements over last year's results.

VoIP Security Responsibility

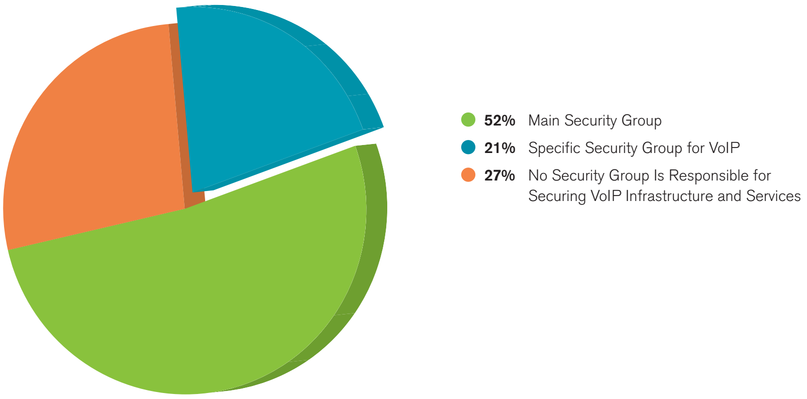


Figure 74 *Source: Arbor Networks, Inc.*

Nearly 80 percent of operators have the ability to detect threats against VoIP infrastructure. Slightly over one-fifth of respondents reported having no visibility. Operators leveraging commercial tools for visibility nearly doubled from last year's report, and the percentage with no visibility dropped by 25 percent from last year's survey. Overall, VoIP infrastructure visibility has significantly improved from last year (Figure 75).

Detection of DDoS Threats Against VoIP Infrastructure

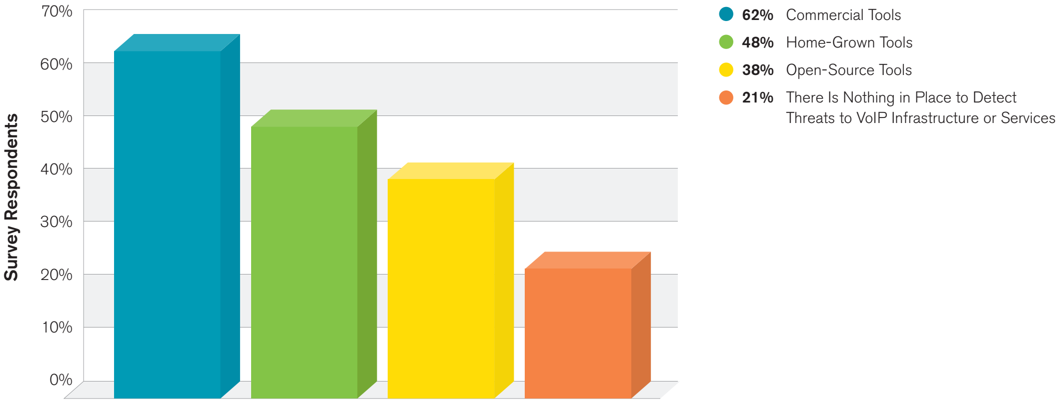


Figure 75 *Source: Arbor Networks, Inc.*

The most commonly deployed mitigation technologies among VoIP operators are firewalls, IDMS, interface ACLs and SBCs (Figure 76). Other tools deployed include: IDS/IPS, FlowSpec, and source- or destination-based remote triggered black holes.

Tools Used to Mitigate DDoS Attacks Against VoIP Services/Infrastructure

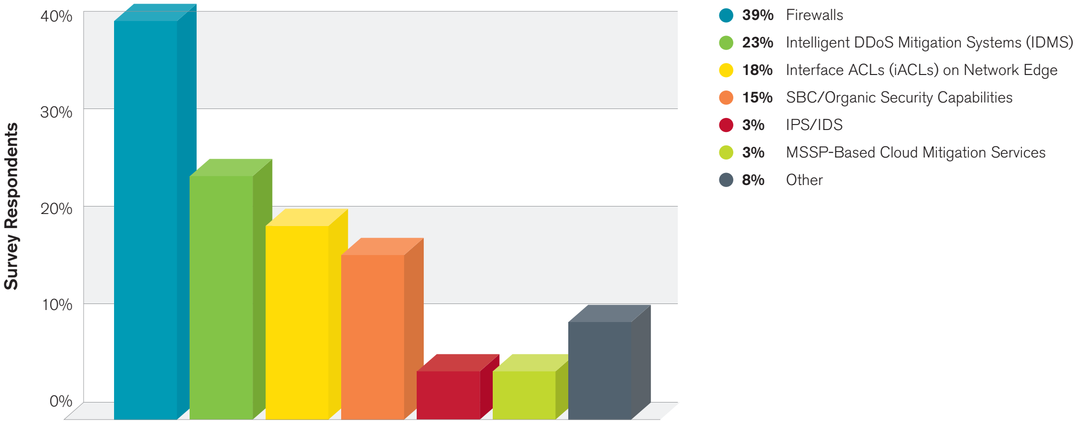


Figure 76 *Source: Arbor Networks, Inc.*

During the survey period, half of the respondents saw incidents of toll fraud attacks against their VoIP networks. Nearly 60 percent saw brute force attacks used to initiate toll fraud, a 30 percent increase over last year's report (Figure 77). Only 44 percent expressed concern for spoofing of caller ID, down from nearly 63 percent in the previous 12 months (Figure 78). This could indicate that improvements were made in the authentication of users within the VOIP networks.

Brute Force Attacks Used to Initiate Toll Fraud

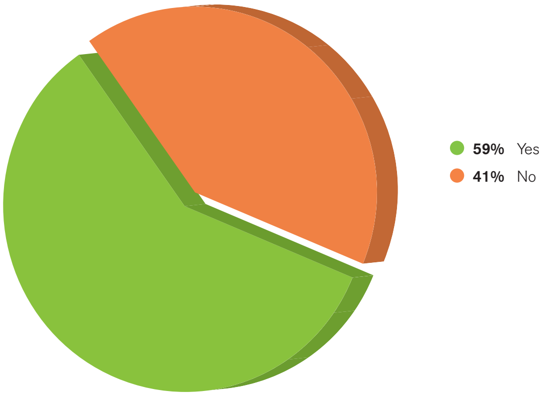


Figure 77 Source: Arbor Networks, Inc.

Concerns Regarding Caller ID Spoofing on VoIP Services

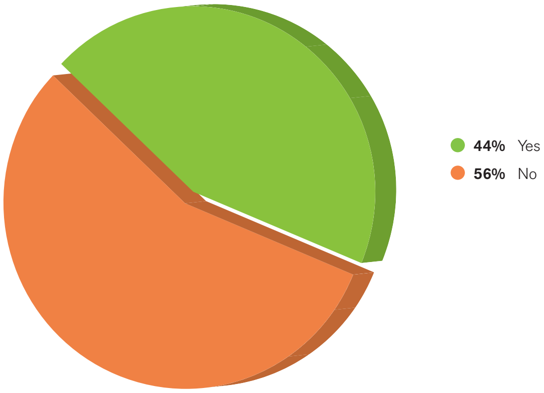


Figure 78 Source: Arbor Networks, Inc.

Approximately two-thirds of VoIP providers indicated they use SBCs. Of those, over 60 percent protect the SBCs with external tools such as firewalls, IDMS and IPS (Figures 79 and 80). These are modest increases over last year, indicating improvements in VoIP infrastructure security.

SBCs Deployed

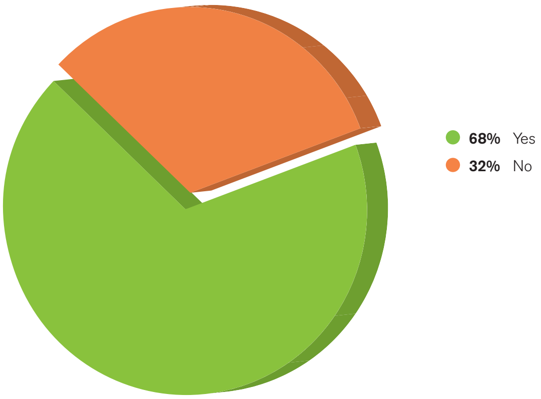


Figure 79 Source: Arbor Networks, Inc.

SBCs Protected by External Tools

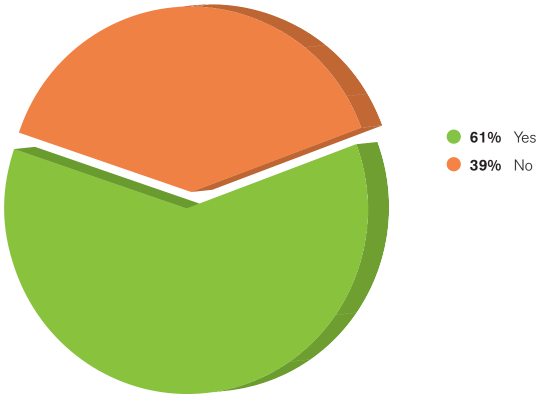


Figure 80 Source: Arbor Networks, Inc.

DNS and DNSSEC Operators

Approximately 19 percent of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security. Seventy-nine percent of respondents have implemented the best practice of restricting recursive lookups by their DNS servers to queries located either on their own networks or on those of their end users, while 21 percent have not yet done so. Just over one-quarter of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period—a significant increase over the 12 percent of respondents from last year's survey.

More than 81 percent of respondents operate DNS servers on their networks. Over 80 percent have either assigned responsibility for their DNS infrastructure to their main OPSEC group or to a dedicated DNS security team (Figure 81). The slight reduction in respondents operating DNS over last year's 87 percent can be attributed to the increased participation from MSSPs and large enterprises this year.

DNS Security Responsibility

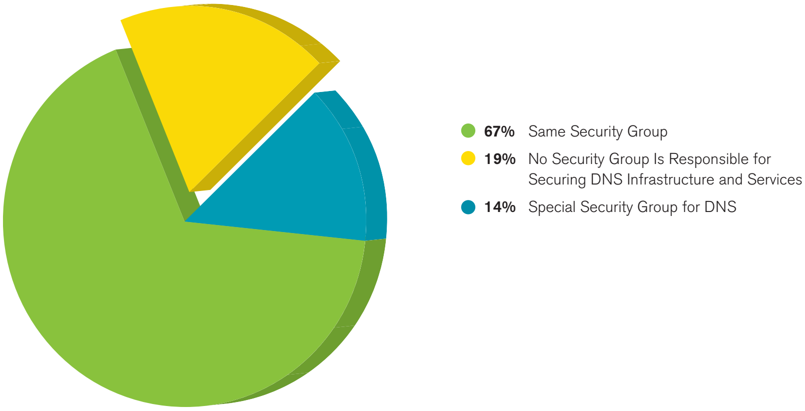


Figure 81 *Source: Arbor Networks, Inc.*

Approximately 19 percent of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security, down from nearly 23 percent last year. While this is a small improvement, the lack of security focus is likely a contributing factor to the significant number of unsecured, open DNS resolvers on the Internet today that can be abused to launch extremely high-bandwidth DNS reflection/amplification attacks.

When asked if they have good visibility of the traffic into or out of their DNS infrastructure, nearly 71 percent of respondents reported good visibility at Layers 3 and 4, while only 27 percent reported Layer 7 visibility (Figure 82).

DNS Traffic Visibility

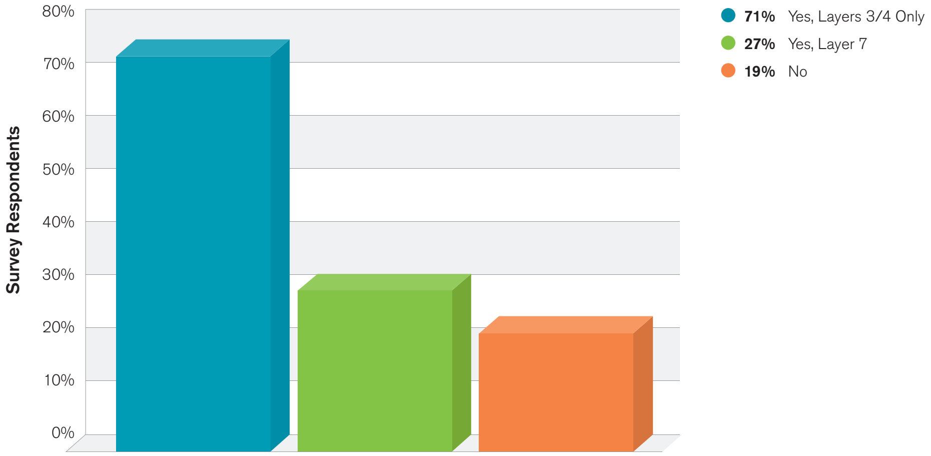


Figure 82 *Source: Arbor Networks, Inc.*

Seventy-nine percent of respondents have implemented the best practice of restricting recursive lookups by their DNS servers to queries located either on their own networks or on those of their end users, while 21 percent have not yet done so (Figure 83). This is an almost identical result to last year's survey. The lack of improvement has allowed large DNS reflective attacks to continue.

DNS Recursive Lookups Restricted

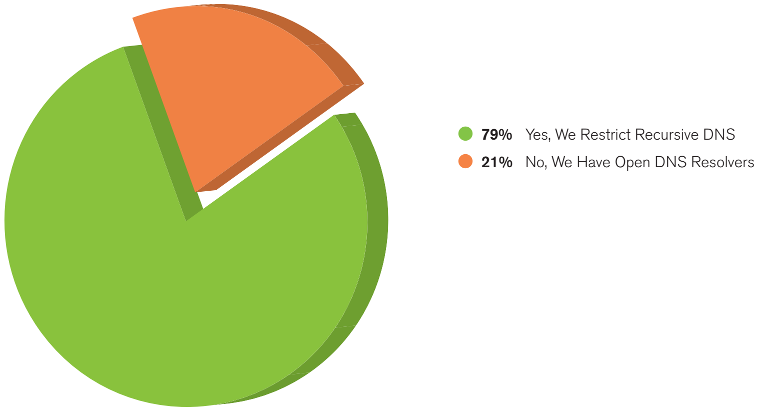


Figure 83 *Source: Arbor Networks, Inc.*

As indicated in Figure 84, just over one-quarter of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period—a significant increase over the 12 percent of respondents from last year's survey. ATLAS statistics corroborate this finding, showing an increase in the proportion of attacks targeting DNS (*ATLAS-Monitored DNS Attacks*, below). Attacking the authoritative DNS servers for a given server or domain is often the easiest way to take it offline. In many cases, it also requires fewer attack resources to disrupt service than would attacking the target servers/applications directly. Collateral damage is a major issue with these kinds of attacks as all of the domains for which it is authoritative may become unresolvable. An attack earlier this year against a DNS registrar based in Europe demonstrated this problem; the authoritative server(s) for a small number of domains were targeted for ideological reasons, leading to a massive number of domains becoming unresolvable.

Customer-Impacting DNS Attacks

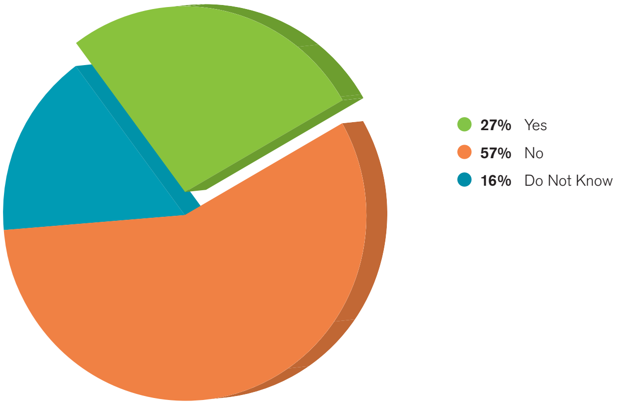


Figure 84 *Source: Arbor Networks, Inc.*

ATLAS-Monitored DNS Attacks

The ATLAS system shows that the proportion of monitored attacks targeting port 53 has increased from 11% through 2011 to 15% in 2012. The average attack targeting DNS services stood at 1.29 Gbps or 1.65 Mpps, with an average attack duration of 6 hours and 37 minutes. However, very large attacks have been seen in 2012—with the largest, tracked by ATLAS, being at 66 Mpps (with multiple others in the 30-40 Mpps range).

As noted in Figures 85 and 86 respectively, nearly 41 percent of respondents indicated they have experienced DDoS attacks against their authoritative DNS servers, while 25 percent indicated they have experienced attacks against their recursive DNS servers during the survey period. This year's responses indicate a significant increase in DNS attacks from last year, rising from 20 percent to 25 percent. Interestingly, over 18 percent of respondents do not know whether they have experienced such attacks during the survey period.

Operators of DNS infrastructure should prioritize improvements to their DNS traffic visibility to ensure the security of this critical service. The following are some respondent descriptions of DNS attacks in the past year:

- "Attacks using our recursive servers for reflection attacks (ANY queries for isc.org and other zones) are very common; thousands of QPS aggregate against several recursive server IPs simultaneously"
- "Both direct and reflected attacks have occurred. They have ranged from 10-100Mbps (most) to 1 Gbps (one)"
- "Direct attack to the DNS servers"

DDoS Attacks Against Authoritative DNS Servers

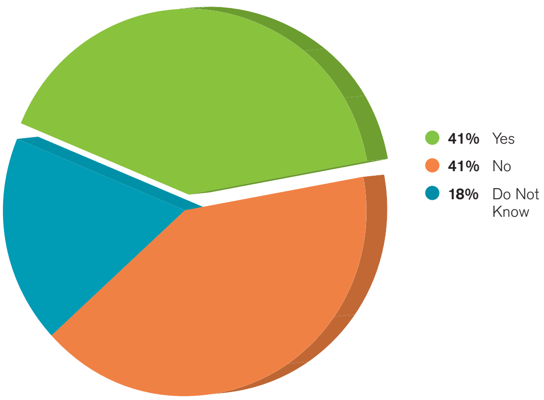


Figure 85 *Source: Arbor Networks, Inc.*

DDoS Attacks Against Recursive DNS Servers

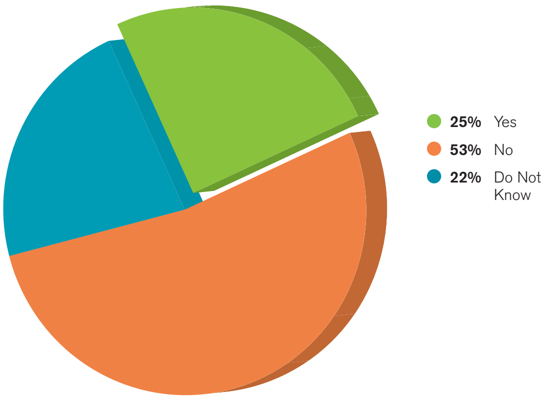


Figure 86 *Source: Arbor Networks, Inc.*

About 18 percent of respondents reported experiencing DNS cache-poisoning attacks directed to, or through, their DNS infrastructures during the survey period (Figure 87). Surprisingly, however, 33 percent indicated that they do not know whether or not they have experienced these attacks, which again reveals that some operators have a serious gap in DNS server traffic visibility. These results reflect almost no change in reported attacks, but a 12 percent decrease in visibility over last year.

DNS Cache-Poisoning Attacks

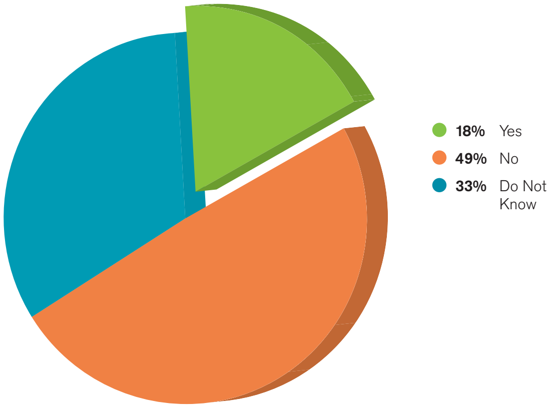


Figure 87 *Source: Arbor Networks, Inc.*

Issues with DNSSEC Functionality

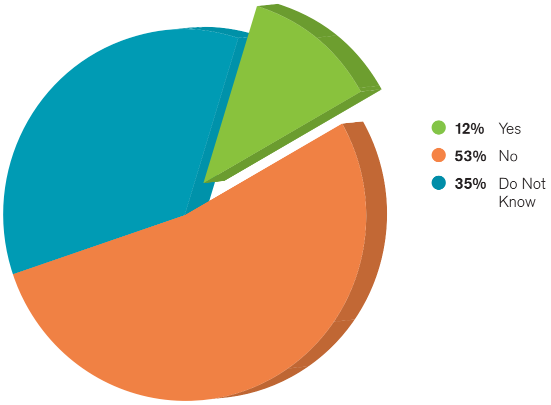


Figure 88 *Source: Arbor Networks, Inc.*

As illustrated in Figure 88, just over half of respondents stated that they did not observe any issues with DNSSEC functionality due to the lack of EDNS0 and/or TCP/53 DNS support on the Internet at large, improving slightly over last year's 46 percent. However, 35 percent still indicated that they have insufficient visibility to make this determination. While this is a significant improvement from 45 percent last year, it still indicates a serious gap in DNS operator traffic analysis capabilities for just over one-third of respondents.

Almost half of respondents indicated that they do not believe drastically increased DNS response sizes have resulted in larger, more damaging DNS reflection/amplification attacks (Figure 89). As noted in last year's report, DDoS attack amplification leveraging DNSSEC has been observed in the wild, in contrast with respondent views. This may be due to a lack of Layer 7 DNS traffic visibility, as mentioned earlier in this section.

Greater Impact Traffic Visibility Solution

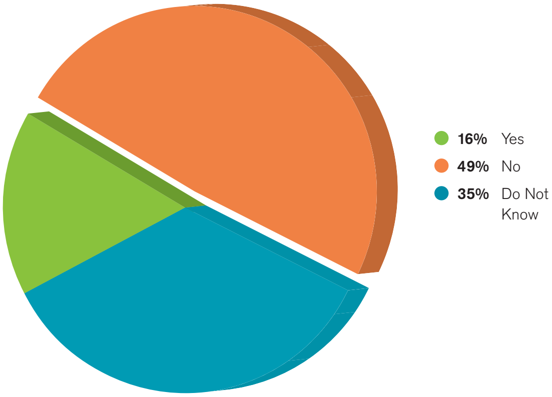


Figure 89 *Source: Arbor Networks, Inc.*

When asked if they had additional concerns regarding DNSSEC deployment, respondents provided the following feedback:

- "Large DNS response size increase as DNSSEC becomes more common and implemented (makes reflection attacks much easier). Increased overhead and processing power required by resolvers."
- "Complexity of DNSSEC will contribute to more outages than security-related incidents. Lack of 'authentication' in DNS (and UDP) provides too easy a method to abuse it for reflection/amplification attack."
- "Misconfigurations causing mail delivery failures, spammers using seemingly valid SPF records to inflate anti-spam scores."
- "Yes, people not deploying it, users not able to validate."

Respondents indicated they are using a variety of security measures and tools to protect their DNS infrastructure from DDoS attack (Figure 90). Over 53 percent indicated they have deployed an IDMS. And over two-thirds have employed iACLs, with significant numbers also using firewalls, IPS/IDS and other measures.

DNS Security Measures

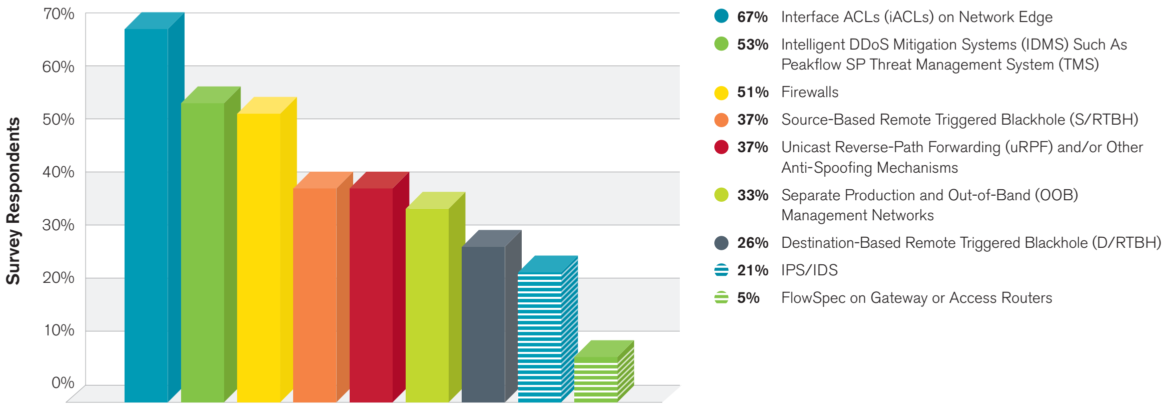


Figure 90 *Source: Arbor Networks, Inc.*

Organizational Security Practices

Figure 91 illustrates that a majority of respondent organizations have implemented best current practices (BCPs) in critical network infrastructure security, once again representing significant progress over last year. These BCPs include routing protocol authentication; iACLs to keep undesirable traffic away from network infrastructure devices; and anti-spoofing measures at the edges of their networks.

Network Infrastructure Security Practices

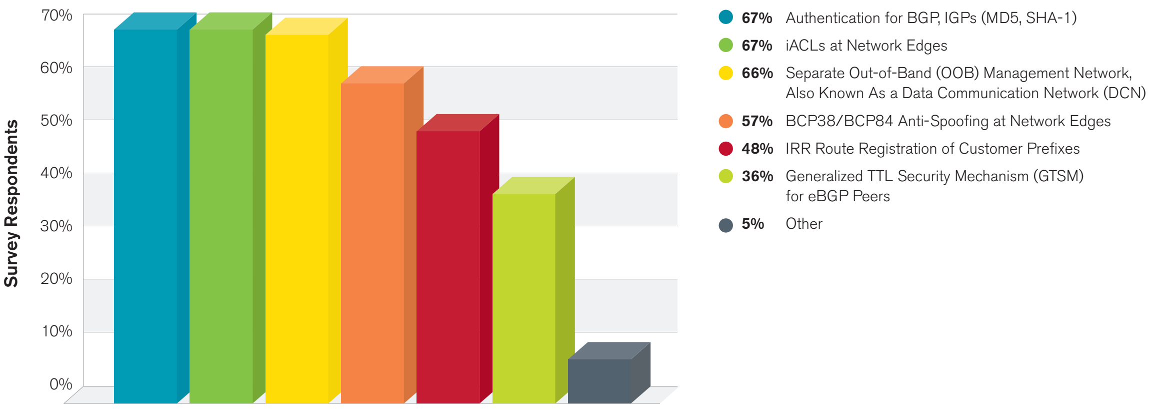


Figure 91 *Source: Arbor Networks, Inc.*

Nearly two-thirds of respondents have implemented out-of-band management networks (also called data communication networks or DCNs) that enable them to retain visibility into and control of their networks even during network partition events. More than 48 percent perform Internet Routing Registry (IRR) registration of their customer routes, up from 38 percent last year.

Response readiness also saw improvement again this year, with 49 percent of respondent organizations practicing DDoS attack and defense simulations for their network. In the last survey, 42 percent of respondents indicated that they exercised their response readiness plans. Approximately 15 percent said they run simulations yearly, and another 26 percent run them either quarterly or monthly (Figure 92). We are very pleased by this development, and believe the improvement is directly related to the increasing number of victims, combined with the fact that the DDoS problem is now a top-of-mind concern for IT executives and their security teams. One organization had this impressive response: “Weekly simulations… with occasional ‘surprise’ simulations on other days. Engineers may also schedule their own intra-team simulations any time/day they choose.”

Attack and Defense Simulations

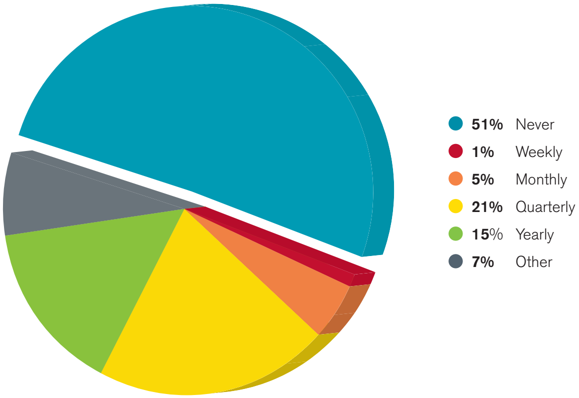


Figure 92 *Source: Arbor Networks, Inc.*

Seventy-six percent of respondents explicitly filter their customer route announcements. This was down slightly from last year. Just over one-half of respondents explicitly filter inbound routing advertisements from peers and upstream transit providers (Figure 93). This is also down slightly from last year. Just over half of respondents now monitor for route hijacking (Figure 94).

Filtering of Route Announcements from Peers

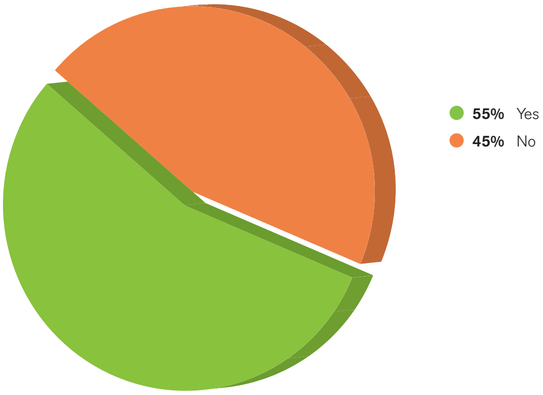


Figure 93 *Source: Arbor Networks, Inc.*

Monitoring for Route Hijacks

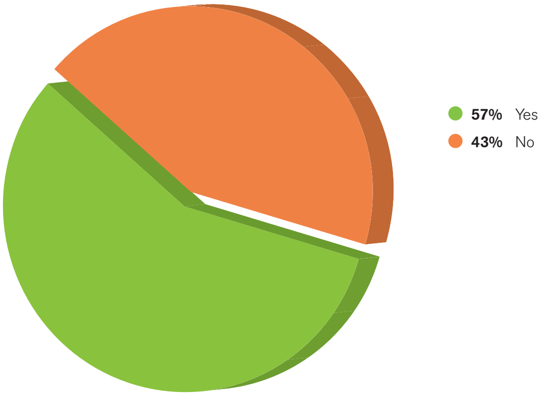


Figure 94 *Source: Arbor Networks, Inc.*

Organizations are using a variety of tools and techniques to correlate disparate events within their infrastructure. SIEM tools are the most common. NMS and internally developed tools also had strong representation.

An interesting—and to an extent unexpected—change is that 41 percent of respondents are now proactively blocking traffic to known botnet C&C servers, malware drop servers, etc. This is a substantial increase from 25 percent last year (Figure 95). This is encouraging, as reducing the number of actively participating devices within a botnet does, to an extent, limit its capability. However, botnets using more sophisticated C&C mechanisms are unlikely to be impacted.

Proactive Blocking of Traffic to Known Botnet C&C

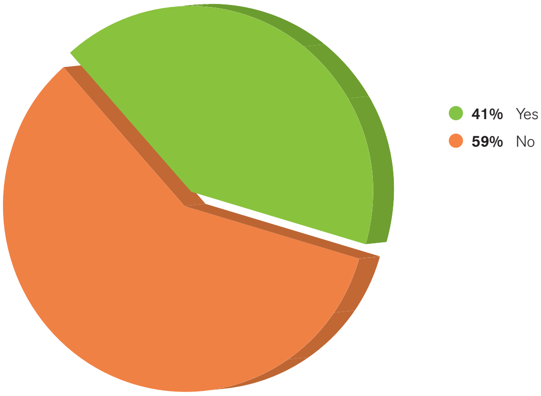


Figure 95 *Source: Arbor Networks, Inc.*

Looking at the sharing of information within the OPSEC community, over 43 percent of respondents indicated that they participate in closed or vetted global OPSEC groups. Eighty-four percent indicated that they believe these groups are highly effective in handling OPSEC issues on an inter-organizational basis. Compared to last year's survey, participation is up slightly, but confidence is marginally down.

Nearly 87 percent of respondents indicated that their OPSEC organizations make it a point to maintain current contact information for the OPSEC teams and/or other empowered groups within their peer, transit provider and customer organizations (Figure 96). This represents a 17 percent improvement over last year and an encouraging sign, as DDoS attacks are sometimes unnecessarily prolonged due to the lack of basic contact information.

Maintaining Contact Information

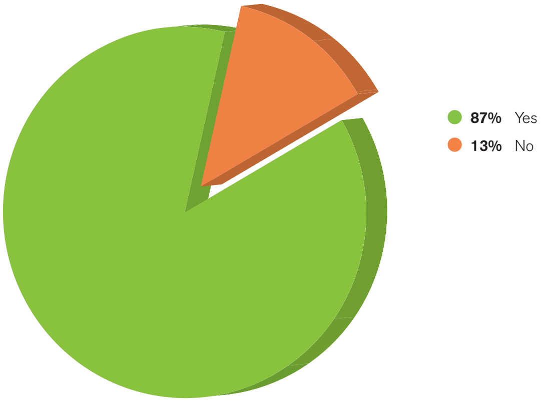


Figure 96 *Source: Arbor Networks, Inc.*

As for building and maintaining OPSEC teams, significant systemic challenges to full participation in closed/vetted global OPSEC groups persist (Figure 97). Lack of time/resources is the most frequently cited challenge, along with lack of management support, policy barriers, unclear benefits and legal concerns.

Barriers to Participation in Security Groups

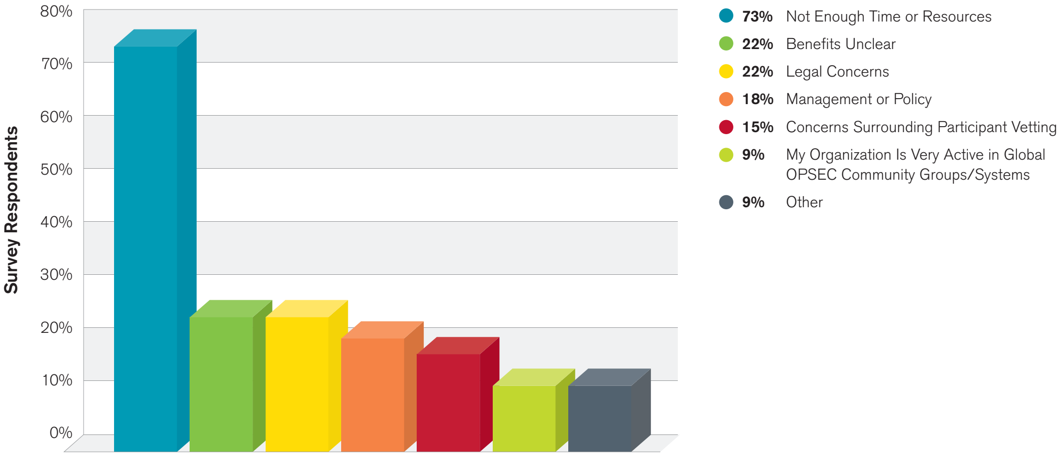


Figure 97 *Source: Arbor Networks, Inc.*

Observations on Law Enforcement, CERTs and CSIRTs

Just over half of respondents indicated that they do not refer security incidents to law enforcement. Overall, confidence in law enforcement efficacy is still relatively low. Over 84 percent of respondents believe that government CERTs/CSIRTs have a positive role to play in OPSEC incident response and welcome their involvement. Two-thirds of respondents are concerned that governments are not doing enough to protect critical network infrastructure.

Just over half of respondents indicated that they do not refer security incidents to law enforcement (Figure 98), a significant decrease from last year's 74 percent. Reasons most cited for not reporting include a lack of resources and time, low confidence in law enforcement investigative efficacy and corporate policy (Figure 99). Some free-form comments from respondents who do not currently make law enforcement referrals follow:

- "Concerns regarding seized equipment"
- "That is the customer's decision"

Referral to Law Enforcement

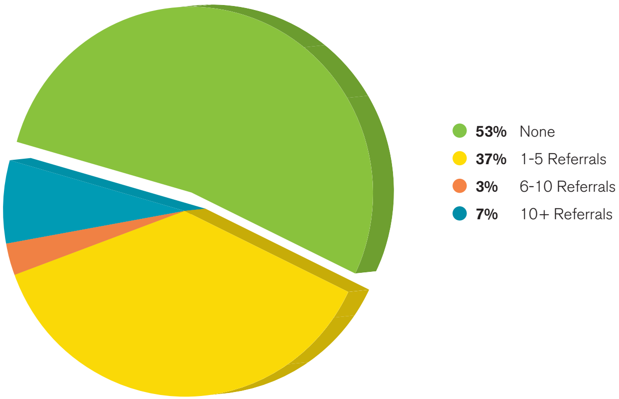


Figure 98 *Source: Arbor Networks, Inc.*

Reasons for Not Referring to Law Enforcement

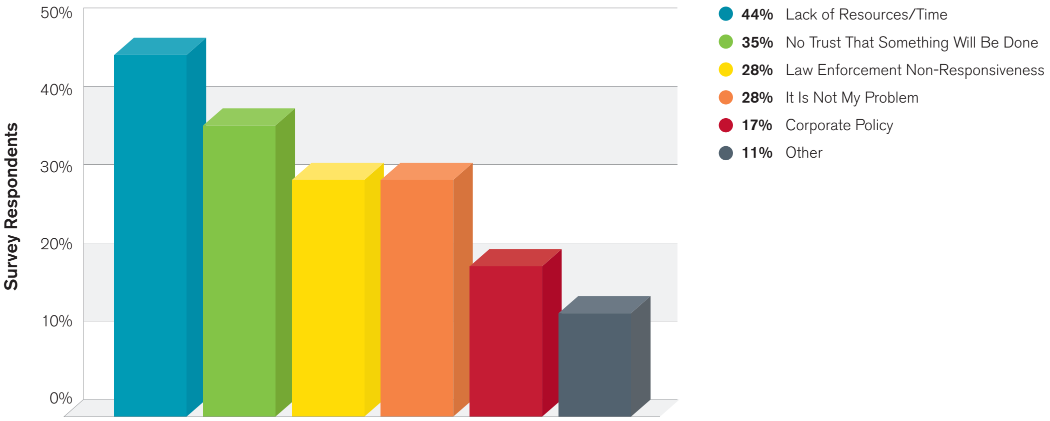


Figure 99 *Source: Arbor Networks, Inc.*

Overall, confidence in law enforcement efficacy is still relatively low. Just under one-third of respondents stated that such law enforcement efforts are effective, while just under one-half stated that they are sometimes effective—similar results to last year. However, fewer organizations see law enforcement becoming more useful to Internet security operations this year, with far more seeing no change (Figure 100). According to respondents in some jurisdictions, legislation and/or regulation require security events to be reported by network operators, irrespective of the ability of the relevant law enforcement agencies to take further action.

Law Enforcement More/Less Useful to Internet Security Operations

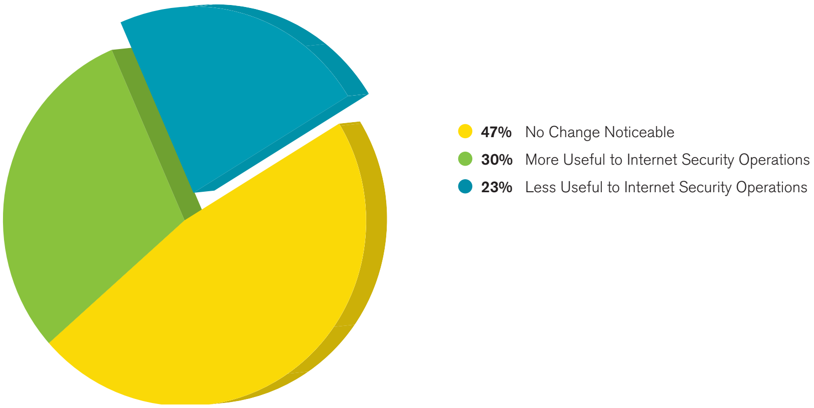


Figure 100 *Source: Arbor Networks, Inc.*

Figures 101 and 102 illustrate that nearly 58 percent of respondent organizations have now established a CERT or CSIRT, and nearly two-thirds are actively engaged with their respective national or regional CERTs and/or CSIRTs. This represents an 18 percent increase in organizations that now have an internal CERT, a major increase from last year's survey.

Organizations with Their Own CERT

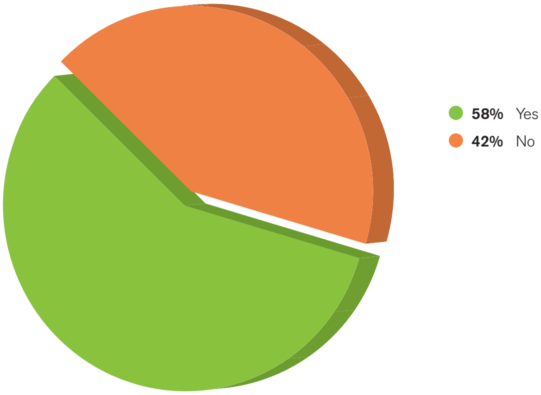


Figure 101 Source: Arbor Networks, Inc.

Organizations Actively Involved with the National or Regional CERT

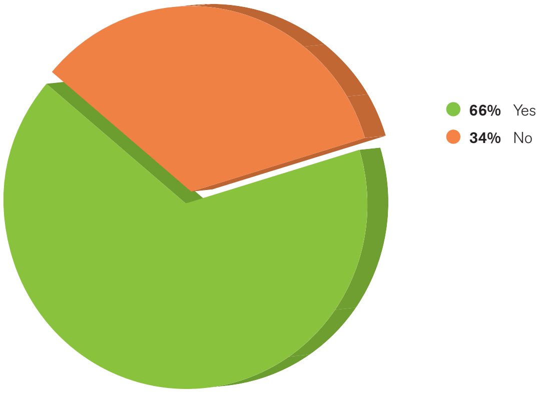


Figure 102 Source: Arbor Networks, Inc.

Over 84 percent of respondents believe that government CERTs/CSIRTs have a positive role to play in OPSEC incident response and welcome their involvement. Two-thirds of respondents are concerned that governments are not doing enough to protect critical network infrastructure (Figure 103). This is an improvement over last year's 73 percent.

Government Effectiveness in Enabling Critical Infrastructure Protection

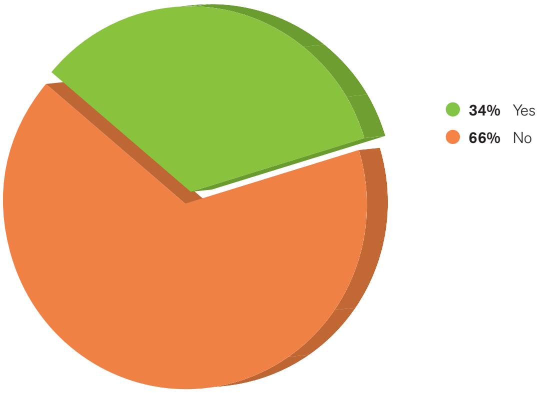


Figure 103 Source: Arbor Networks, Inc.

Four of every five respondents indicated they have concerns about sharing details of their security information outside of their own organization. But significantly fewer respondents have concerns sharing the same information outside of their community or region (Figure 104). The results here are broadly similar to last year, although there has been an approximate 10 percent decrease in the proportion of respondents who are concerned about sharing details outside of their region.

Concerns About Sharing Information

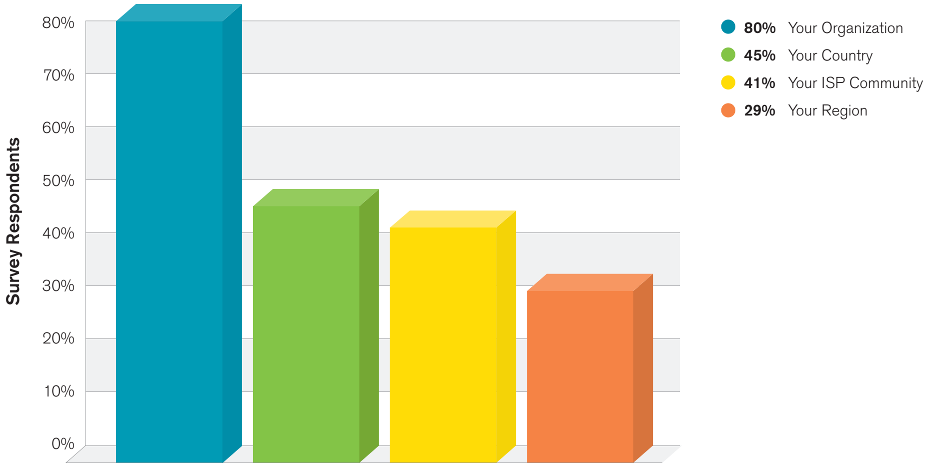


Figure 104 *Source: Arbor Networks, Inc.*

Slightly more than 20 percent of respondents indicated they are aware of laws, regulations or codes of practices in their operating jurisdictions that mandate DDoS defenses (Figure 105). However, nearly half indicated there are no such requirements for protection from this type of service availability threat.

Regulatory Requirements

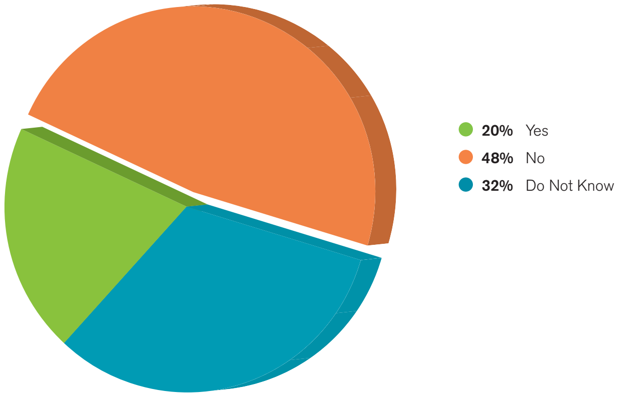


Figure 105 *Source: Arbor Networks, Inc.*

Infrastructure Security in the Enterprise

Nearly 90 percent of respondents indicated they provide services to customers, partners or employees that are accessible via the Internet. Sixty-two percent of enterprises stated that any interruption to these services would have a significant impact to the business.

This year's survey captured information specific to enterprise customers in the following fields: financial services, gaming, e-commerce, healthcare, manufacturing and utilities. Nearly 90 percent of respondents indicated they provide services to customers, partners or employees that are accessible via the Internet (Figure 106).

Enterprises Providing Internet-Accessible Services

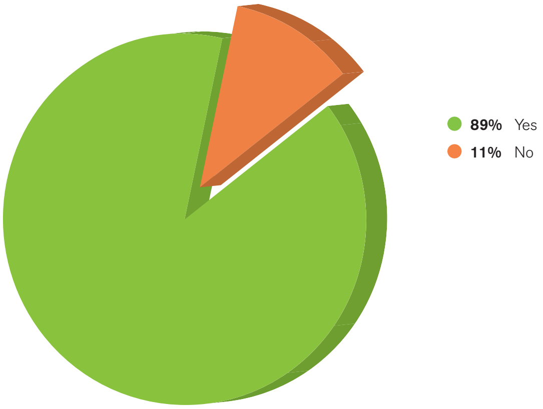


***Figure 106** Source: Arbor Networks, Inc.*

While all the respondents indicated they host Internet-accessible services within the enterprise infrastructure, one-quarter said they also host Internet-accessible services in private Internet data centers. Sixty-three percent reported utilizing shared Internet data centers or hosting facilities (Figure 107).

Hosted Internet Services (Locations)

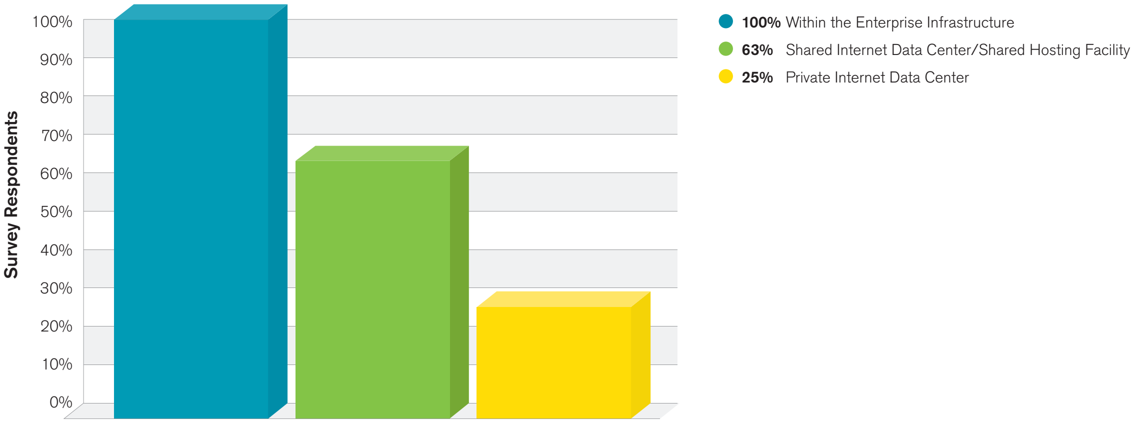


Figure 107 Source: Arbor Networks, Inc.

Sixty-three percent of enterprises stated that any interruption to these services would have a significant impact to the business. All respondents indicated there would be at least some impact to their business if Internet-accessible services were interrupted (Figure 108). Not surprisingly, 88 percent indicated their Internet-accessible services are covered by some sort of SLA or regulatory framework (Figure 109).

Business Impact from Interruption of Service

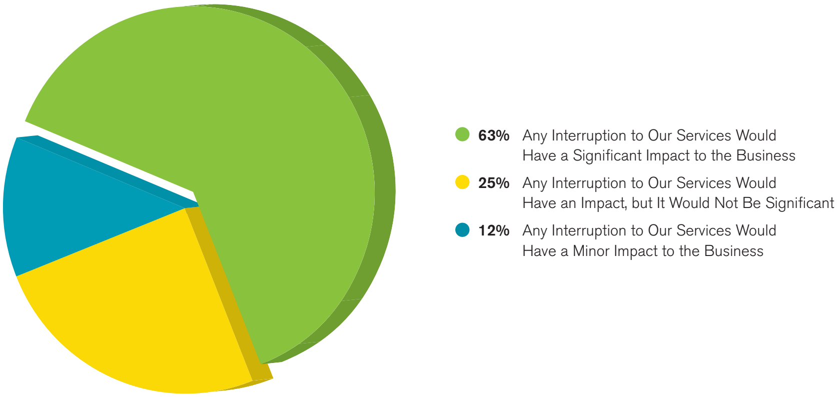


Figure 108 Source: Arbor Networks, Inc.

Internet Services Covered by SLA

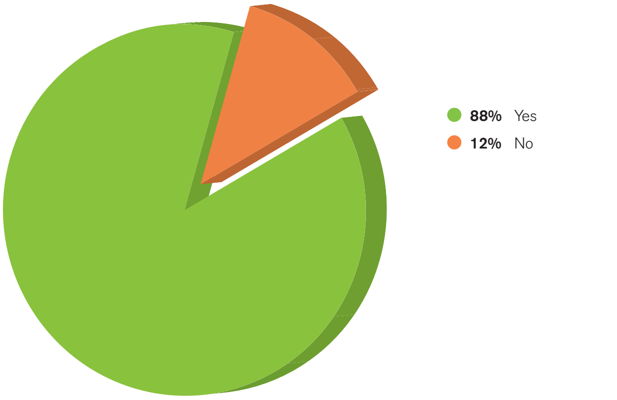


Figure 109 *Source: Arbor Networks, Inc.*

Sixty-three percent of enterprise respondents said they have good visibility into the traffic to and from their Internet-accessible services (Figure 110).

Good Traffic Visibility

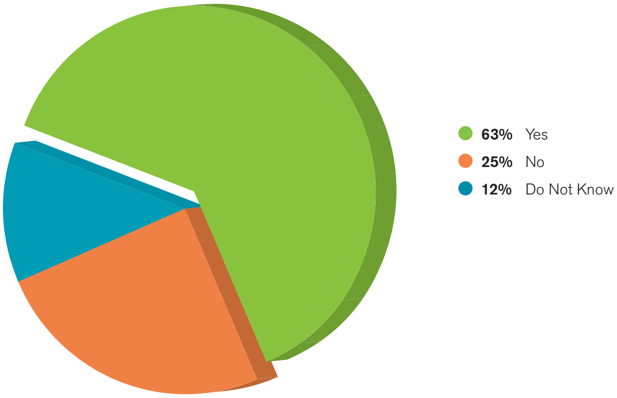


Figure 110 *Source: Arbor Networks, Inc.*

The vast majority of respondents have traffic visibility from counters and statistics on their infrastructure. Half of them use a flow-based monitoring solution, and over one-third are using vendor-supplied monitoring tools, third-party monitoring solutions or service provider portals (Figure 111).

How Visibility Is Provided

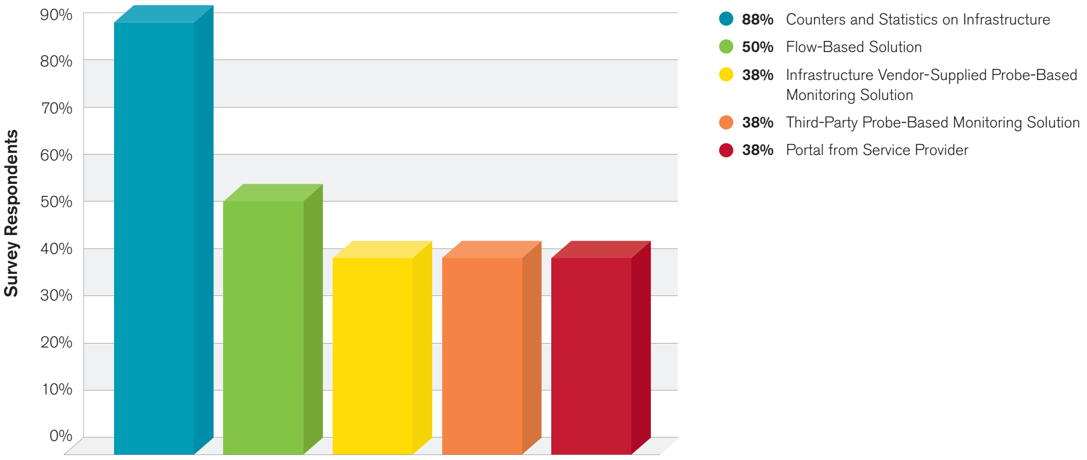


Figure 111 *Source: Arbor Networks, Inc.*

Enterprise Threats and Concerns

Half of the respondents indicated they have experienced DDoS attacks against their infrastructure, and one-quarter encountered DDoS attacks against customer- and partner-facing services during the 12-month survey period. On a more encouraging note, 50 percent of respondents confirmed that DDoS is a part of their business risk management process for Internet service availability. Over 62 percent of respondent enterprise organizations allow employees to utilize their own devices on the corporate network but twenty-five percent reported that they do not have anything currently deployed which allows them to monitor or identify these devices.

Half of the respondents indicated they have experienced DDoS attacks against their infrastructure, and one-quarter encountered DDoS attacks against customer- and partner-facing services during the 12-month survey period (Figure 112). Concerns about threats in the next 12 months were high across the board—with DDoS attacks clearly top-of-mind, along with data exfiltration and under-capacity (Figure 113).

DDoS Attacks in the Last Year

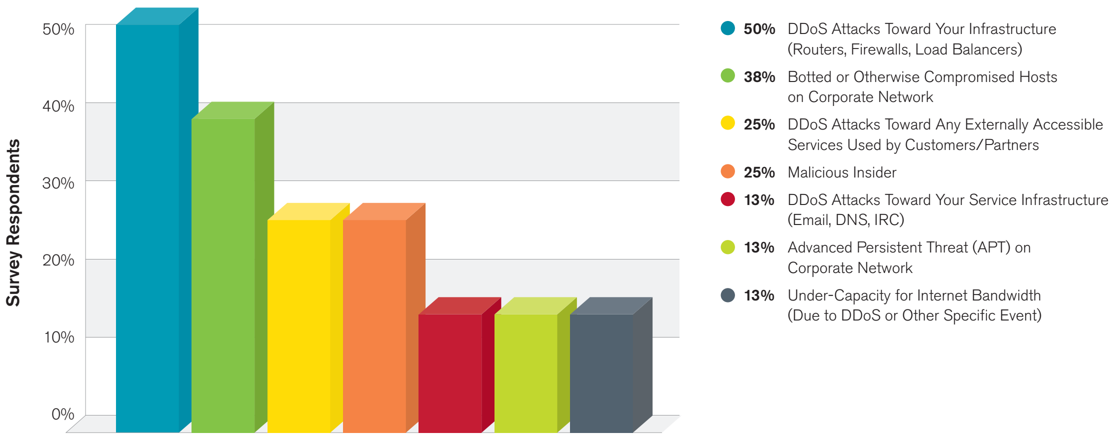


Figure 112 *Source: Arbor Networks, Inc.*

Threat Concerns Over the Next 12 Months

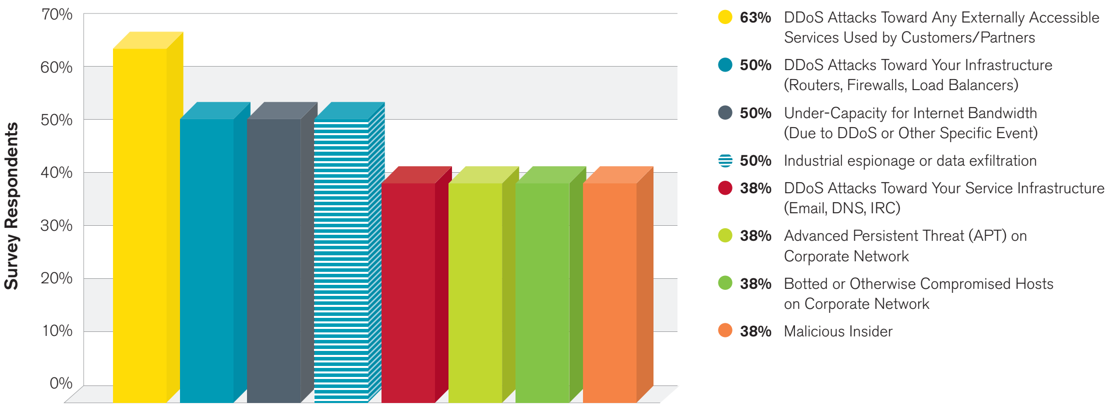


Figure 113 *Source: Arbor Networks, Inc.*

Enterprise respondents are using a wide variety of tools to detect threats against their organizations. While the most commonly used tools are firewalls and IDS, many respondents are also using SNMP-based tools, flow analyzers and in-house developed tools (Figure 114).

Tools Used to Detect Threats

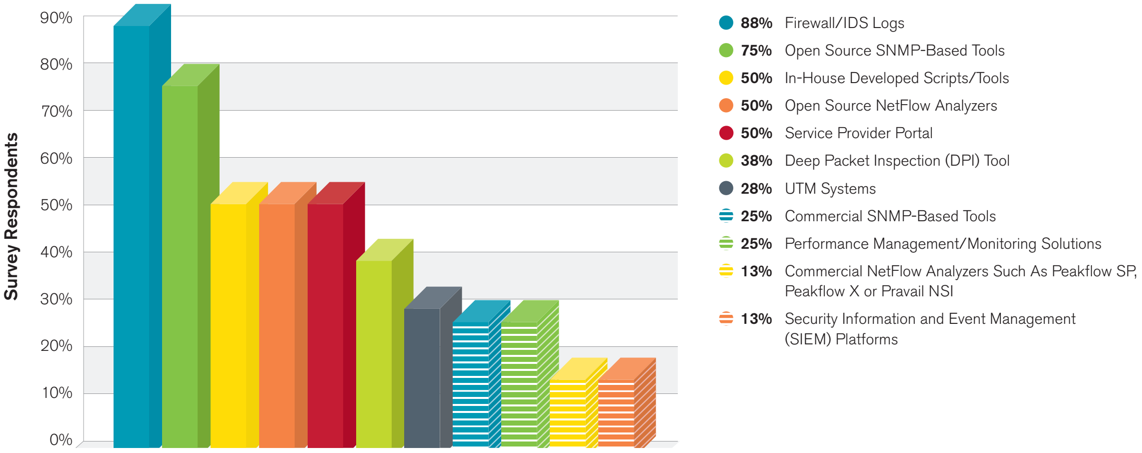


Figure 114 *Source: Arbor Networks, Inc.*

Interestingly, only 37 percent saw an increased awareness of the DDoS threat in their organization over the last 12 months (Figure 115). Given the continued mainstream press coverage of attacks, this is a lower figure than expected. In contrast, more than half of service provider respondents saw increased awareness both within their own organizations and within their customers' organizations. One reason for this may be that the responding segments (who are Arbor customers and high-priority segments likely to be attacked) already had high awareness.

Awareness of the DDoS Threat in the Enterprise

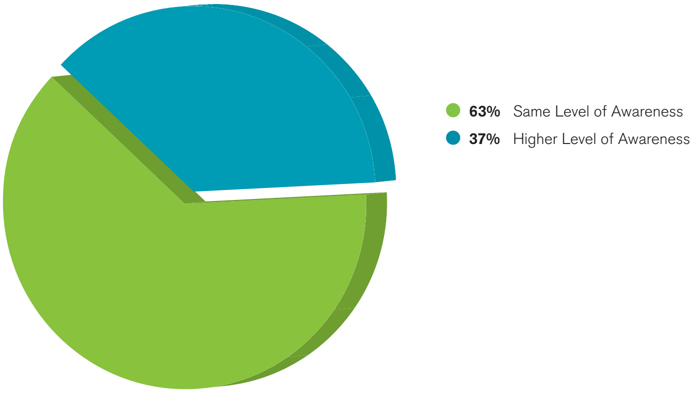


Figure 115 *Source: Arbor Networks, Inc.*

When citing reasons for this change, the most common response was "financial/legal liability assessment." Other reasons cited were "experienced one or more DDoS attacks," "highly-publicized DDoS attacks such as Wikileaks/ Anonymous," "business continuity planning risk assessment," "brand reputation concerns," and "legislative/regulatory requirements." One respondent summed it up with this comment: "No specific event has risen the awareness, it is just a slow ongoing cultural process."

Half of all enterprise respondents stated that C-level executives within the organization are not aware of the threat DDoS attacks pose to Internet service availability (Figure 116). This is a concern and may indicate that the business impact of DDoS attacks has not yet been fully appreciated within some organizations.

C-Level Awareness of the DDoS Threat

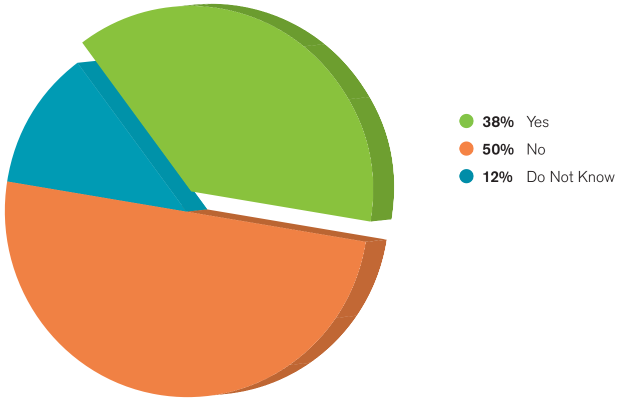


Figure 116 *Source: Arbor Networks, Inc.*

On a more encouraging note, 50 percent of respondents confirmed that DDoS is a part of their business risk management process for Internet service availability. This is in addition to traditional concerns such as fire protection, power stability and physical access.

In this year's survey, questions were added regarding areas of current discussion within the OPSEC community, such as social media, BYOD, etc. Considering the explosive growth of social media in recent years, it is not surprising that three-quarters of enterprise respondents allow the use of social media. However, around one-quarter of respondents do not allow—and even actively prevent—its usage.

With the continued proliferation of smartphones and tablets, BYOD is an ever-growing trend in the enterprise that presents multiple challenges and opportunities for employers and employees alike. Over 62 percent of respondent enterprise organizations allow employees to utilize their own devices on the corporate network. However, only half of respondents allow the use of public cloud services to synchronize data between organization- and employee-owned devices.

Enterprises are using a variety of methods to monitor and detect employee-owned devices. The most common response was "network access control systems," while others are using "host-based posture assessment" and "flow-based monitoring systems." Twenty-five percent reported that they do not have anything currently deployed (Figure 117).

BYOD Monitoring

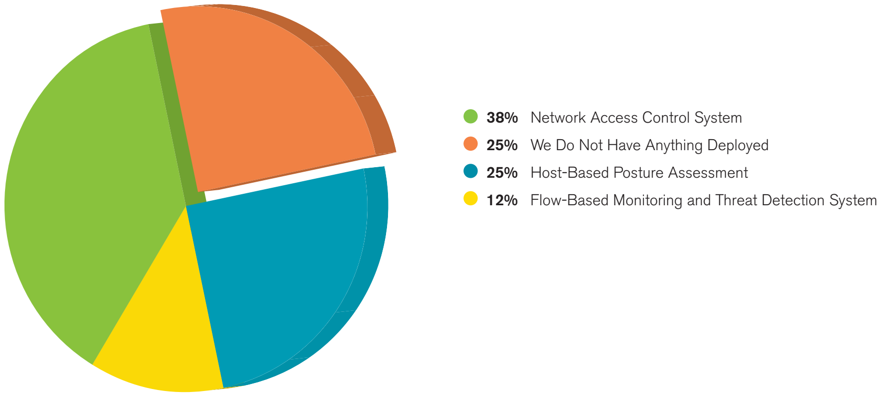


Figure 117 *Source: Arbor Networks, Inc.*

In terms of security breaches, one-eighth of respondents reported incidents attributed to employee-owned devices being used on the enterprise network.

Seventy-five percent of respondents are using firewalls or IPS devices to mitigate DDoS attacks in the enterprise. Many are also leveraging their service providers for DDoS mitigation (Figure 118). The shortcomings of firewalls and IPS devices when dealing with DDoS attacks are well-known and discussed earlier in this report.

DDoS Mitigation Capabilities in the Enterprise

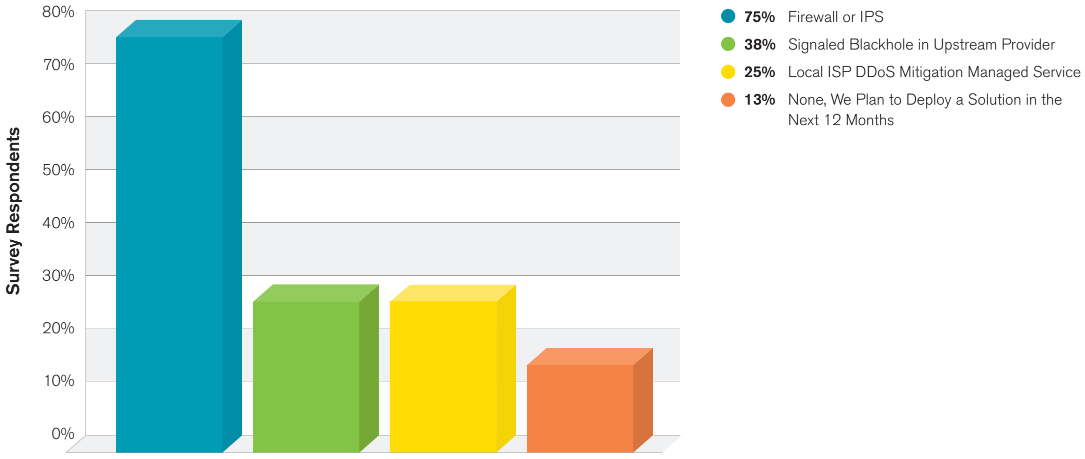


Figure 118 *Source: Arbor Networks, Inc.*

Enterprise respondents who evaluated DDoS mitigation services found the price of the service and the mitigation capacity to be the two most important factors. Other considerations were evenly split among: SLA for mitigation activation time, access to experienced SOC personnel, guarantee that redirected traffic stay in region, service provided by local ISP, vendor equipment used and brand reputation of provider (Figure 119).

Priorities When Selecting DDoS Mitigation Service

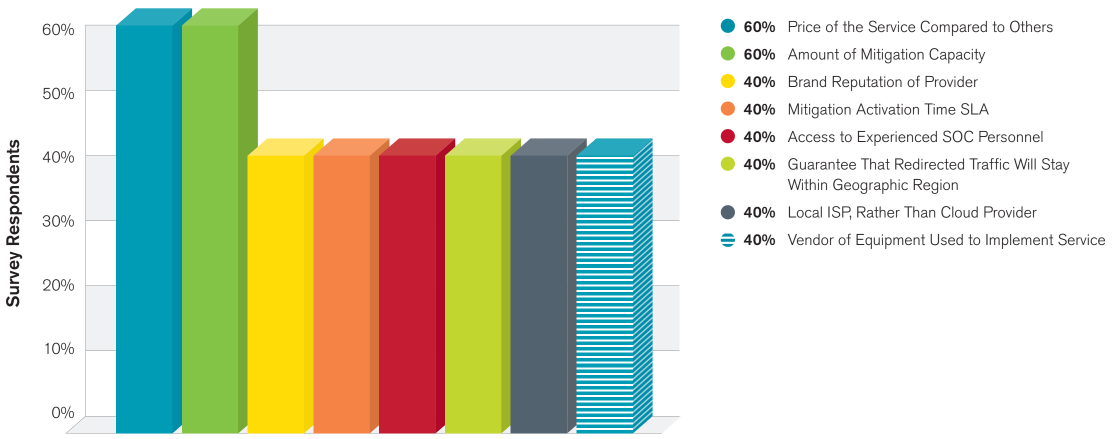


Figure 119 *Source: Arbor Networks, Inc.*

Conclusions

Arbor Networks' 2011 *Worldwide Infrastructure Security Report* (published in January 2012) shed new light on a host of issues. In this year's report we see additional and emerging threats. We see new trends developing and existing ones confirmed. Let's take a closer look at some of the most interesting findings.

Advanced Persistent Threats a Top Concern for Operators and Enterprises

Advanced Persistent Threats are a well-established problem in the enterprise. This year's survey found that they are a top-of-mind concern for network operators as well. This year we found an increased level of concern over botted or compromised machines on service provider networks. This may indicate that infected hosts are causing problems for operators as well as enterprises. The increase in botted hosts is not surprising given the number and complexity of malware variants that exist, their rate of evolution and the consequent inability of IDS and AV systems to fully protect against them. Looking ahead, there is even more concern about APT, industrial espionage, data exfiltration and malicious insiders.

Bring Your Own Device (BYOD) Trend Creates New Challenges

In the growing trend commonly referred to as BYOD, half of respondents now allow personal devices on their networks. However, only 40 percent have a means to monitor usage of these hosts. Additionally, only 13 percent actively block access to social media applications and sites. Clearly, BYOD is creating more entry-points for hackers to enter the network.

DDoS: Attack Sizes Plateau in Trend Toward Complex Multi-Vector Attacks

This year's results confirm that application-layer and multi-vector attacks are continuing to evolve in terms of complexity while the largest volumetric attacks are starting to plateau in size.

Application-layer attacks have become increasingly common over the past few years, with 86 percent of our respondents reporting these more sophisticated attacks targeting Web services. More alarmingly though, 46 percent of respondents are reporting multi-vector attacks. These attacks employ combinations of volumetric, state-exhaustion and application-layer attack vectors targeting an organization at the same time. This is a marked increase from last year's report where just 27 percent reported these attacks. Multi-vector attacks can be challenging to mitigate and generally require layered solutions across the data center and the cloud for successful mitigation—which is why they are an attractive approach for hackers looking to cause the most damage. The fourth quarter 2012 attacks targeting U.S. financial services institutions are an excellent example of multi-vector attacks. As of the final production of this document, these attacks were still underway.

Data Centers Are Increasingly Victimized

Nearly 50 percent of respondents experienced DDoS attacks toward their data centers during the survey period, and 94 percent of these respondents report seeing DDoS attacks regularly. Nearly 90 percent of data center operators suffering DDoS attacks reported operational expenses as a business impact due to the attacks.

As more companies move their services to the cloud, they now have to be wary of the shared risks and the potential for collateral damage. With e-commerce and online gaming sites being the most common targets, according to survey results this year, sharing data centers with these organizations brings some risk.

DDoS Motivations

Last year we reported for the first time that ideology was the most common motivation for DDoS attacks, and this trend has clearly continued through 2012 as reflected in this year's report. The top three most common perceived motivations for DDoS attacks are:

- Political/ideological (i.e., hacktivism)
- Online gaming
- Vandalism/nihilism

These are largely personally motivated—acts done in reaction to real or perceived offenses.

Mobile Providers Continue to Be Reactive

There has been limited improvement in visibility and investment in detection and mitigation solutions specific to the mobile network since the last survey. For example, a full 60 percent of respondents do not have visibility into the traffic on their mobile/evolved packet cores. The economics of consumer subscriber networks do not incent providers to implement security until a problem occurs.

The advancing adoption of LTE deployments and wireless services in general significantly increases the reach of broadband Internet access to a much larger user base. Additionally, it allows mobile devices to become the primary means of Internet access for users given the increased available bandwidth. As mobile providers continue to increase capacity faster than visibility and threat detection capabilities, security problems are likely.

DNS Infrastructure Remains Vulnerable

Approximately 19 percent of respondents indicate that there is no security group within their organizations with formal responsibility for DNS security. When asked if they have good visibility of the traffic into or out of their DNS infrastructure, nearly 71 percent of respondents reported good visibility at Layers 3 and 4 but only 27 percent reported Layer 7 visibility. The fact that 21% of respondents still do not restrict access to DNS recursors, combined with poor visibility and a lack of dedicated security personnel, provides an environment for attackers to exploit.

IPv6 Deployments Becoming Pervasive

Last year we saw our first reports of IPv6 DDoS attacks on production networks. We noted that even though IPv6 DDoS attacks were being reported, IPv6 security incidents were still relatively rare. Considering that 75 percent of respondents are service providers, it's no great surprise that IPv6 deployments are accelerating. Fully 80 percent of respondents have partial or full IPv6 deployments already, with most implemented as dual stack. This opens new opportunities for attackers to bypass network controls by switching between IPv4 and IPv6 networks.

Law Enforcement Still Not Engaged but Readiness Improving

Just over half of respondents still do not refer security incidents to law enforcement; this is actually a significant decrease from last year's 74 percent. So while the perennial disengagement of most network operators from law enforcement continues, it's an improvement from previous years. Overall, confidence in law enforcement efficacy is still relatively low with just under a third of respondents stating they are effective, and with just under half stating that they are sometimes effective—similar results to last year.

Readiness, on the other hand, is improving. Forty-nine percent of respondent organizations now practice DDoS attack and defense simulations compared to only 42 percent last year. Roughly 15 percent run simulations yearly and another 26 percent run them quarterly or monthly. Clearly the DDoS problem is now a top-of-mind concern for IT executives and their security teams, more so than in years past. This is a positive step in staying ahead of attackers and one that is directly related to the increasing number of victims this past year.

About the Authors

Darren Anstee, Solutions Architect for EMEA, Arbor Networks

danstee@arbor.net

Darren Anstee has over 15 years of experience in the pre-sales, consultancy and support aspects of telecom and security solutions. Currently in his eighth year at Arbor, Anstee specializes in customizing and supporting traffic monitoring and Internet threat detection and mitigation solutions for service providers and enterprises in the EMEA region. Prior to joining Arbor, he spent eight years working in both pre- and post-sales for core routing and switching product vendors.

Dick Bussiere, Solutions Architect for APAC, Arbor Networks

dbussiere@arbor.net

Dick Bussiere is a seasoned technical architect with over 20 years of experience in ICT security, computer networking and engineering. As Arbor Networks Solution Architect for the Asia Pacific region, Bussiere is responsible for ensuring that Arbor's product roadmap meets the needs of the region and for evangelizing DDoS risks and remediation techniques and technologies. He frequently assists Internet service providers, financial institutions and governments in assessing their risk exposure to DDoS attacks and in developing policies and methodologies to deflect these attacks. He has advised several regulatory bodies on recommended legislation to protect critical infrastructure against DDoS attacks.

Prior to joining Arbor, Bussiere was a principle in an ICT security consulting firm and provided consulting services to numerous business, academic and government organizations. He was also an active contributor to the IEEE P1901 Power Line Communication security architecture and specification and an active participant in the IEEE and IETF working groups. Bussiere is currently the holder of five patents related to computer networking.

Gary Sockrider, Solutions Architect for the Americas, Arbor Networks

gsockrider@arbor.net

Gary Sockrider is the Arbor Networks Solutions Architect for the Americas. He seeks to understand and convey the constantly evolving threat landscape as well as the techniques and solutions that address them. He works across the organization to ensure customers experience an optimal deployment and their needs and interests are best represented.

Sockrider is an industry veteran with over 20 years of broad technology experience ranging from routing and switching to network security, data center and collaboration. He has diverse experience in multiple roles including Support, IT, Security SME and Product Management. Prior to joining Arbor Networks, Sockrider spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.

CONTRIBUTORS

Carlos Morales, Vice President, Systems Engineering and Sales Operations

cmorales@arbor.net

Carlos Morales is responsible for pre-sales technical support, design, consulting and implementation services for Arbor customers and partners worldwide. He is also responsible for sales approvals, sales processing, maintenance contracts, forecasting, data analysis and reporting for Arbor. Morales works closely with Arbor's customers and strategic and integration partners to ensure ongoing product interoperability and to set the direction for new product features. He has more than 15 years of experience implementing security, routing and access solutions in service provider, cloud and enterprise networks. Morales' background includes management positions at Nortel Networks, where he served as the director of systems engineering for Nortel's access products. Formerly, he was systems engineering director for Tiburon Networks and held systems engineering roles at Shiva Corporation, Crescent Networks and Hayes Microcomputer.

Glossary

A

ACL	Access Control List
APT	Advanced Persistent Threat
ASERT	Arbor Security Engineering & Response Team
ATLAS	Active Threat Level Analysis System
AV	Anti-Virus

B

BCP	Best Current Practice
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device

C

C&C	Command-and-Control
CAPEX	Capital Expenditure
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CPE	Customer Premises Equipment
CSIRT	Computer Security Incident Response Team

D

DCN	Data Communication Network
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
D-RTBH	Destination-based Remotely Triggered Blackholing
S-RTBH	Source-based Remotely Triggered Blackholing

E

EDNS0	Extension Mechanisms for DNS

G

Gbps	Gigabits-per-second
Gi	Global Internet
GSM	Global System for Mobile

H

HTTP	Hypertext Transfer Protocol
HTTP/S	HTTP Secure

I

iACL	Infrastructure ACL
ICMP	Internet Control Message Protocol
IDC	Internet Data Center
IDMS	Intelligent DDoS Mitigation System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRR	Internet Routing Registry

L

LAN	Local Area Network
LOIC	Low Orbit Ion Canon
LTE	Long Term Evolution

M

Mbps	Megabits-per-second
MSS	Managed Security Service
MSSP	Managed Security Service Provider

Glossary (continued)

N

NAT	Network Address Translation
NMS	Network Management System

O

OOB	Out of Band
OPEX	Operational Expenditure
OPSEC	Operational Security

P

PAT	Port Address Translation
PHP	Hypertext Preprocessor

Q

QoE	Quality of Experience

R

RAN	Radio Access Network

S

SBC	Session Border Controller
SIEM	Security Information Event Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SPF	Sender Policy Framework
S/RTBH	Source-based Remotely Triggered Blackholing
SYN	Synchronize

T

TCP	Transmission Control Protocol

U

UDP	User Datagram Protocol

V

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

W

WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe

T +44 207 127 8147

Asia Pacific

T +65 6299 0695

www.arbornetworks.com

SR/WISRI/EN/0113