Arbor Special Report

Worldwide Infrastructure Security Report

2011 Volume VII

ARBOR NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for next-generation data centers and carrier networks. Arbor's proven solutions help grow and protect our customers' networks, businesses and brands. Arbor's unparalleled, privileged relationships with worldwide service providers and global network operators provide unequalled insight into and perspective on Internet security and traffic trends via the ATLAS®—a unique collaborative effort with 100+ network operators across the globe sharing real-time security, traffic and routing information that informs numerous business decisions. For technical insight into the latest security threats and Internet traffic trends, please visit our Web site at www.arbornetworks.com and our blog at asert.arbornetworks.com.

Table of Contents

List of Figures

Overview

Arbor Networks, in cooperation with the broader operational security community, has completed the seventh edition of an ongoing series of annual security surveys. This survey, covering roughly a 12-month period from October 2010 through September 2011, is designed to provide industry-wide data to network operators.

This data is intended to enable more informed decisions about the use of network security technology to protect mission-critical Internet and other IP-based infrastructure. The survey output serves as a general resource for the Internet operations and engineering community, recording information on the employment of various infrastructure security techniques and other trends. It also provides the direct observations, insights and anecdotal experiences of respondents that may be of value to others.

Operational network security issues—the day-to-day aspects of security in commercial networks—are the primary focus of survey respondents. As such, the results provided in this survey are intended to more accurately represent real-world concerns rather than the theoretical and emerging attack vectors addressed and speculated about elsewhere.

Key Findings

Ideologically-Motivated 'Hactivism' and Vandalism Are the Most Readily-Identified DDoS Attack Motivations

A new and extremely important finding in the 2011 *Worldwide Infrastructure Security Report* points to the 'why' behind DDoS attacks. Ideology was the most common motivating factor for DDoS attacks in 2011, followed by a desire to vandalize. When this is coupled with the fact that anyone can be attacked, and anyone can initiate an attack, it is clear a sea-change in the risk assessment model for network operators and end-customers is required. Today, increased situational awareness has become a necessity for all Internet-connected organizations.

- 35% reported political or ideological attack motivation
- 31% reported nihilism or vandalism as attack motivation

10 Gbps and Larger Flood-Based DDoS Attacks Are the 'New Normal'

During the survey period, respondents reported a significant increase in the prevalence of flood-based DDoS attacks in the 10 Gbps range. This represents the "mainstreaming" of large flood-based DDoS attacks, and indicates that network operators must be prepared to withstand and mitigate large flood attacks on a routine basis.

The largest reported DDoS attack during the survey period was 60 Gbps, in contrast with the 100 Gbps attack reported in the previous report. Attacks of this magnitude continue to constitute an extremely serious threat to network infrastructure and ancillary support services such as DNS, not to mention end-customer properties.

Increased Sophistication and Complexity of Application-Layer (Layer 7) DDoS Attacks and Multi-Vector DDoS Attacks Are Becoming More Common

Application-layer (Layer 7) DDoS attacks continue to grow in both prevalence and sophistication. Respondents indicated that sophisticated application-layer DDoS attack methodologies have become commonplace, and that complex multi-vector DDoS attacks with both flood-based and application-layer attack components are rapidly gaining in popularity with attackers.

Visibility and Security of Mobile and Fixed Wireless Networks Are an Ongoing Concern

A significant minority of mobile and fixed wireless operators report continuing challenges to detection of security threats on their networks. The majority of respondents indicated that their network visibility was much stronger than it was in 2010; however, their general lack of ability to detect infected hosts and the wide-spread data concerning attacks point to significant blind spots still resident in their capabilities.

First-Ever Reports of IPv6 DDoS Attacks 'in the Wild' on Production Networks

For the first time, respondents to this year's survey indicated that they had observed IPv6 DDoS attacks on their networks. This marks a significant milestone in the arms race between attackers and defenders, and confirms that network operators must have sufficient visibility and mitigation capabilities to protect IPv6-enabled properties.

Rarity of IPv6-Enabled Attacks Indicates Low IPv6 Market Penetration and Lack of Critical Mass

Even though IPv6 DDoS attacks are now being reported, IPv6 security incidents are relatively rare. This is a clear indication that while IPv6 deployment continues to advance, IPv6 is not yet economically or operationally significant enough to warrant serious attention by the Internet criminal underground. This also indicates that much of the IPv6 network traffic may be un-monitored, masking the real threats on IPv6 networks.

Stateful Firewalls, IPS and Load-Balancer Devices Continue to Fall Short on DDoS Protection Capabilities

Respondents continue to report that stateful firewalls and IPS devices are failing under DDoS attacks due to state-table exhaustion, and report similar findings with regard to load-balancer devices. Network operators must have the capability to defend these stateful devices against DDoS attacks if they are deployed in front of Internet facing services.

The Overwhelming Majority of Network Operators Do Not Engage Law Enforcement for Security Incident Response and Follow Up

The perennial disengagement of most network operators from law enforcement continues, with network operators continuing to lack confidence in law enforcement's capabilities and willingness to investigate online attack activity. Respondents also continue to evince strong dissatisfaction with current governmental efforts to protect critical infrastructure.

Demographics of Survey Respondents

Survey participants included 114 self-classified Tier 1, Tier 2 and other IP network operators (Figure 1) from the U.S. and Canada, Latin/South America, EMEA, Africa and Asia (Figure 2).

This year's respondent pool shows roughly the same demographic distribution of service provider categories as last year's report.

Organizational Type

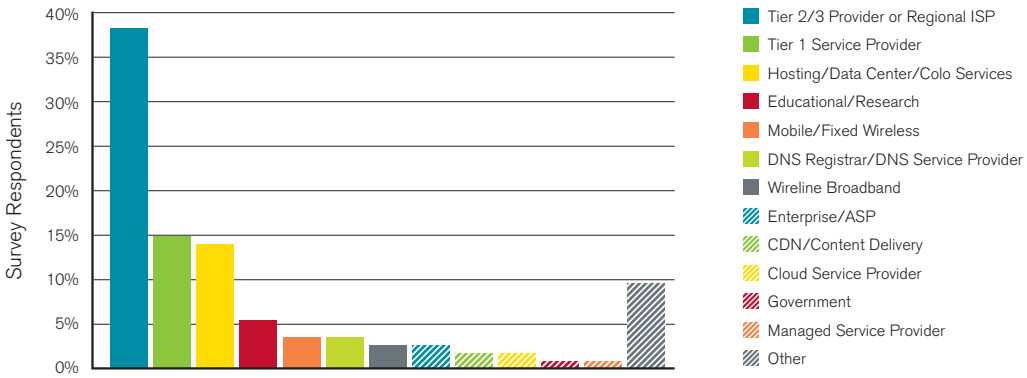

Figure 1 *Source: Arbor Networks, Inc.*

While the number of respondents increased slightly from the 2010 survey, geographical diversity (Figure 2) and operational focus diversity (Figure 3) remained relatively the same year over year.

Geographic Distribution of Organizational Headquarters

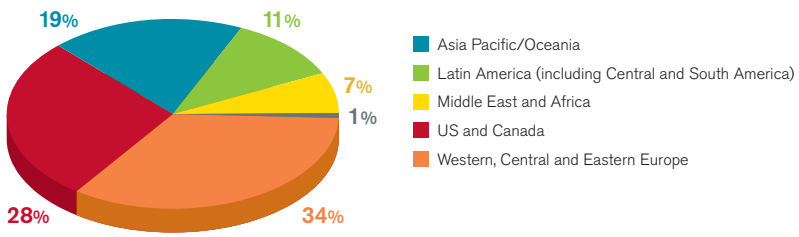

Figure 2 *Source: Arbor Networks, Inc.*

Geographic Coverage of Network

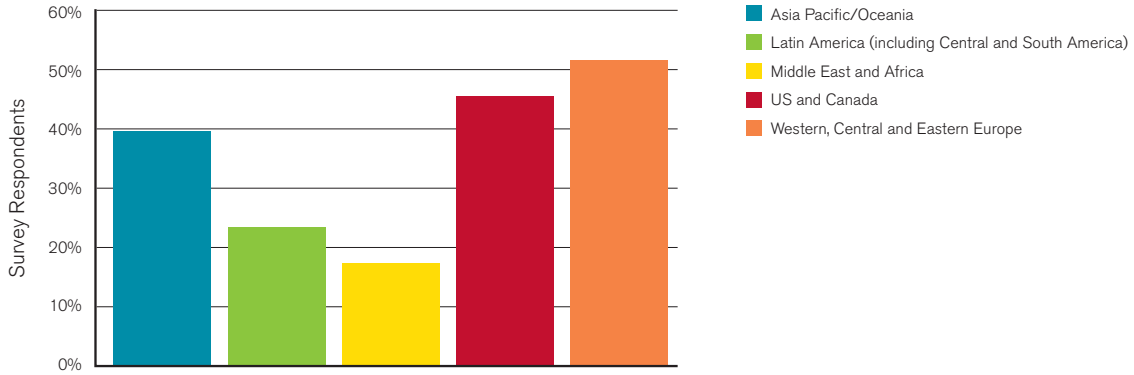

Figure 3 *Source: Arbor Networks, Inc.*

All survey participants are directly involved in network security operations at their respective organizations (Figure 4) and/or make direct contributions to the global operational security community. Once again, the diversity of geographical presence and operational focus has an impact on various results and observable trends over the seven-year survey lifetime—something we attempt to highlight accordingly where considered pertinent.

Role of Respondent

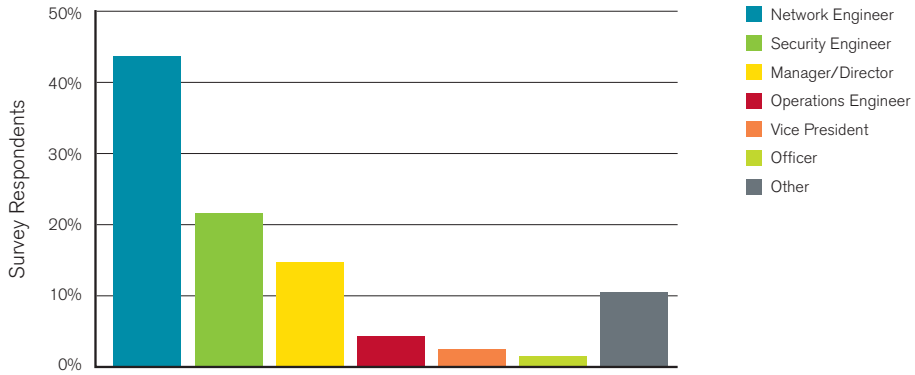

Figure 4 *Source: Arbor Networks, Inc.*

A strong plurality of respondents self-identified their specific job role as that of network engineer, while security engineers and managers were represented in second and third places, respectively. In addition to the titles listed in Figure 4, other job categories included security architects, security analysts, security researchers and managed security services product managers.

Figure 5 illustrates that nearly 32 percent of respondents offer mobile/fixed wireless broadband access and more than 42 percent offer managed security services. In addition to the specific services described in Figure 5, some respondents also offer video-on-demand (VOD) services, e-government-focused services, IPv6 tunnel-broker services and Extensible Provisioning Protocol (EPP) registry services.

Services Offered

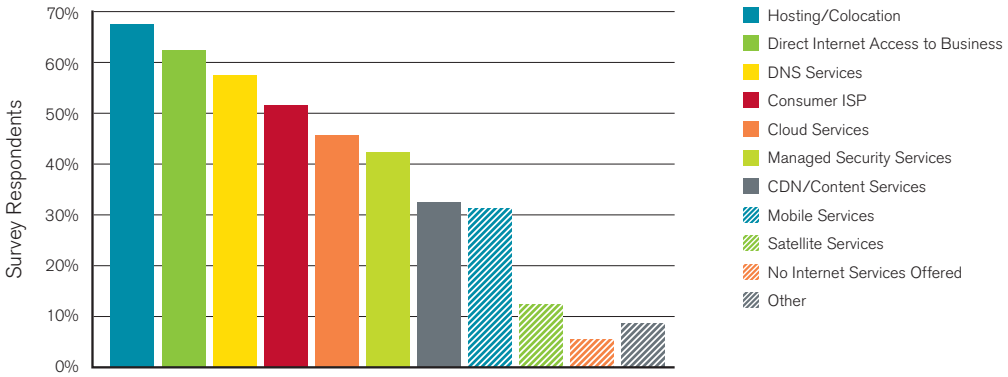

Figure 5 *Source: Arbor Networks, Inc.*

Survey Methodology

The survey consisted of 132 free-form and multiple-choice questions, representing the array of issues facing network operators today. Questions addressed such topics as threats against backbone infrastructure and individual customers; techniques employed to protect network infrastructure itself; and mechanisms used to manage, detect and respond to security incidents.

The survey also included questions specific to data center operators, IPv6 security evolution, managed services, VoIP, DNS, as well as mobile and fixed wireless operators. All data is presented in an aggregated and anonymous manner and provided with the permission of the respondents. Standard mathematical methods to weight responses have been applied where incomplete answers were provided for a given question. Several refinements occurred in this edition of the survey, primarily based on respondent feedback. Some questions were deleted, some added and many simply honed in an attempt to capture the most pertinent data sets.[1]

[1] As in previous reports, several survey questions included multiple selections.

Several questions were added based upon suggestions by respondents to a previous survey, or as a result of direct feedback from one of the many network security and operations forums from which survey review was expressly solicited.

Arbor Networks intends to continue conducting this survey annually and sharing the results with the global Internet security and operations communities. Our goals are:

1. To continually refine the questionnaire in order to provide more timely, detailed and relevant information in future editions.
2. To increase the scope of the survey respondent pool to provide greater representation of the global Internet network operations community.

Most Significant Operational Threats

More than 71 percent of respondents indicated that DDoS attacks toward end customers were a significant operational threat encountered during this 12-month survey period (Figure 6).

Most Significant Operational Threats

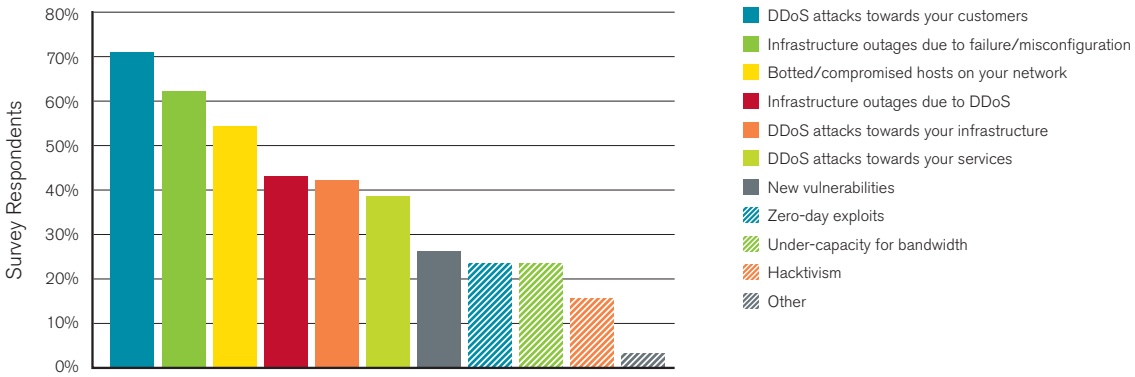

Figure 6 *Source: Arbor Networks, Inc.*

Over 62 percent also identified misconfigurations and/or equipment failures as contributing to outages during the survey period. Botnets and their unwanted effects (including DDoS attacks) were rated highly, as were DDoS attacks targeted at operators' network infrastructure and ancillary support services, such as DNS, Web portals and email servers. Spam and VoIP-related attacks were included in the "Other" category.

With regards to application-layer attacks (Figure 7), respondents listed HTTP, DNS and SMTP as the most-frequently targeted applications, with HTTP/S and SIP/VoIP coming in at fourth and fifth place, respectively. The percentage of HTTP and IRC increased slightly year over year since 2010. DNS, SNMP, HTTP/S and SIP/VoIP decreased slightly over the same period. Targeted applications in the "Other" category include SSH, online gaming, FTP, Telnet, RDP, SQL databases, IRC, PHP and TCP port 123.

Application-Layer DDoS Attacks

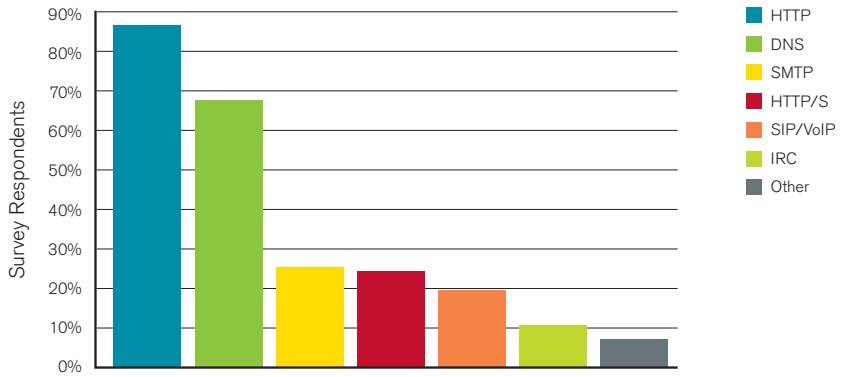

Figure 7 *Source: Arbor Networks, Inc.*

Figure 8 shows that while HTTP GET and HTTP POST were the most common application-layer DDoS attack vectors, more sophisticated mechanisms such as Slowloris, LOIC, Apache Killer, SIP call-control floods, SlowPost and HOIC are increasingly prevalent.

Application-Layer DDoS Attack Methodologies

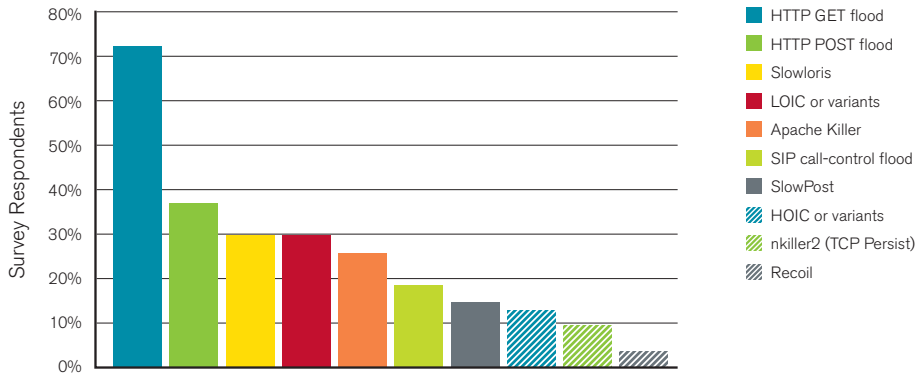

Figure 8 *Source: Arbor Networks, Inc.*

Top security concerns for the next 12 months (Figure 9) include: attacks against end customers; attacks against operators' network infrastructure devices and ancillary support services such as DNS and Web portals; botnet activities, which include DDoS attacks; and, as in last year's report, new vulnerabilities.

Security Concerns

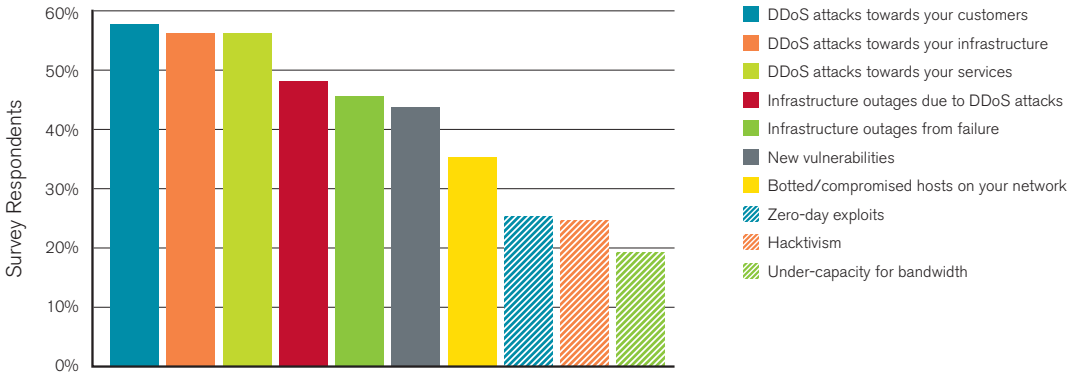

Figure 9 *Source: Arbor Networks, Inc.*

Based upon responses described later, we believe that the prominently highlighted concern over new vulnerabilities continues, at least in part, to be related to the deployment of IPv6. Other forward-looking security concerns expressed include VoIP-specific attacks and data loss or leakage due to botnet and/or malicious insider activity.

While there has been much speculation in the press surrounding possible concerns about the integrity of network infrastructure equipment sourced from various countries, these concerns are not strongly reflected in our findings. Figures 10 and 11 indicate that the overwhelming majority of respondents do not view this as a serious issue, and it appears to have little impact on product procurement decisions, echoing last year's findings.

Concerns Regarding Integrity of Infrastructure Vendor Products

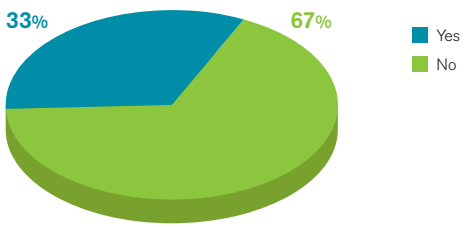

Figure 10 *Source: Arbor Networks, Inc.*

Influence of Integrity Concerns on Product Procurement

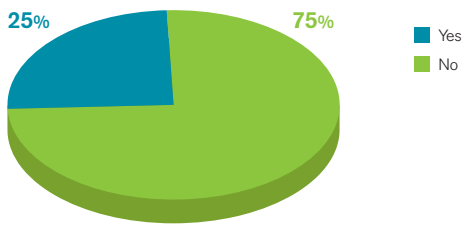

Figure 11 *Source: Arbor Networks, Inc.*

Respondents who indicated concerns regarding product origins offered the following comments:

- "We are not directly concerned, but our customers are."
- "Recently, word-of-mouth advice from regulators suggests we avoid equipment originating from nations perceived as hostile."
- "'Intelligence' is being built into what used to be low-level equipment, like media converters and so on. Couple this with the ubiquity of Internet access, and it makes backdoor access a lot more of a risk."
- "Will not buy boxes with hard-coded support passwords."
- "There are certain vendors that from a global view are either not preferred from a security perspective or have to achieve specific internal accreditation."

By way of contrast, nearly 75 percent of respondents (Figure 12) indicated that the purported geopolitical origin of traffic ingressing and traversing their networks has a significant impact on their perception of the threat that this traffic may pose to their organization and/or end customers.

Influence of Geopolitical Origin of Network Traffic on Threat Perception

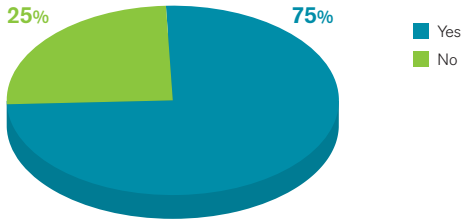

Figure 12 *Source: Arbor Networks, Inc.*

Figure 13 indicates that awareness of DDoS attacks amongst end-customer organizations has greatly increased over the last 12 months. Unfortunately, as seen in Figure 14, the most common reason for this raised awareness is that they have been the target of a DDoS attack. This emphasizes the point that many network operators are ignoring the news about increased attack activity until they themselves fall victim.

DDoS Threat Awareness

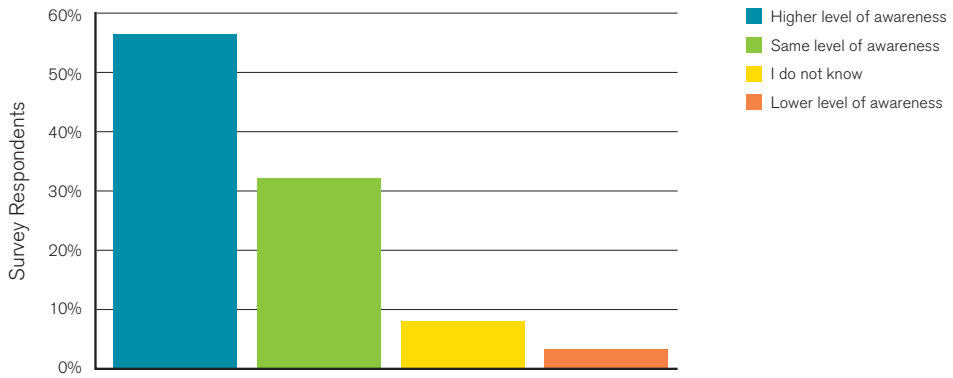

Figure 13 *Source: Arbor Networks, Inc.*

Factors Impacting DDoS Threat Awareness

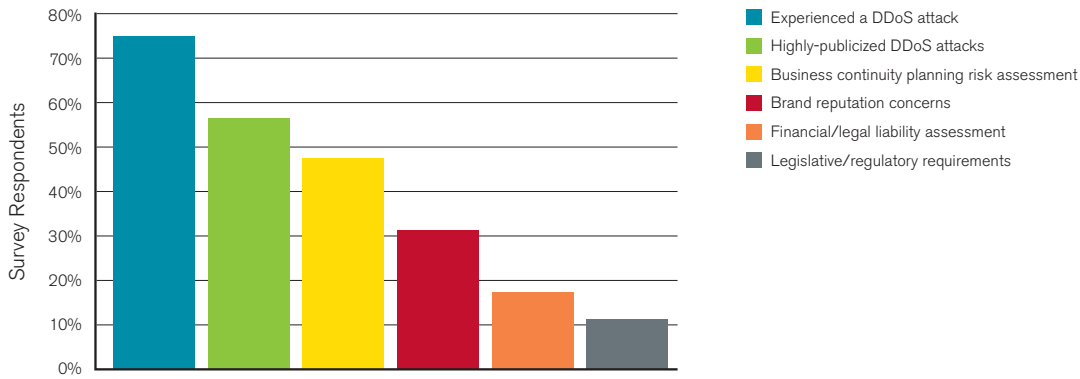

Figure 14 *Source: Arbor Networks, Inc.*

Scale, Targeting and Frequency of Attacks

During the survey period, respondents reported a significant increase in the prevalence of flood-based DDoS attacks in the 10 Gbps range. This represents the "mainstreaming" of large flood-based DDoS attacks, and indicates that network operators must be prepared to withstand and mitigate large flood attacks on a routine basis.

As illustrated in Figure 15, the highest-bandwidth attack observed by respondents during the survey period was a 60 Gbps DNS reflection/amplification attack. This represents a 40 percent decrease from the previous year in terms of sustained attack size for a single attack.

Largest Bandwidth Attacks Reported

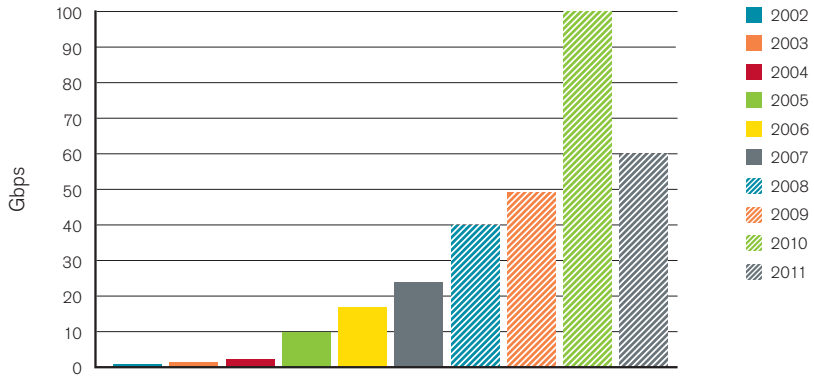

Figure 15 *Source: Arbor Networks, Inc.*

Based upon our experiences working with operators over the last year and data collected using Arbor's ATLAS® portal, we believe that this apparent decrease in attack magnitude at the high end does not represent a significant reduction of risk from flood-based DDoS attacks. Sixty Gbps is a very large attack, and the increased prominence of 10 Gbps and higher attacks reflected in survey responses indicates that the volume of traffic in large-scale flood attacks remains a significant risk.

Over 74 percent of respondents reported that the highest-bandwidth DDoS attack they experienced during this survey period was directed at their end customers, while nearly 13 percent reported that their own ancillary support services such as DNS and Web portals were targeted (Figure 16). Almost 11 percent indicated that their own network infrastructure was the target of the highest-bandwidth attack they experienced.

Target of Highest-Bandwidth DDoS Attack

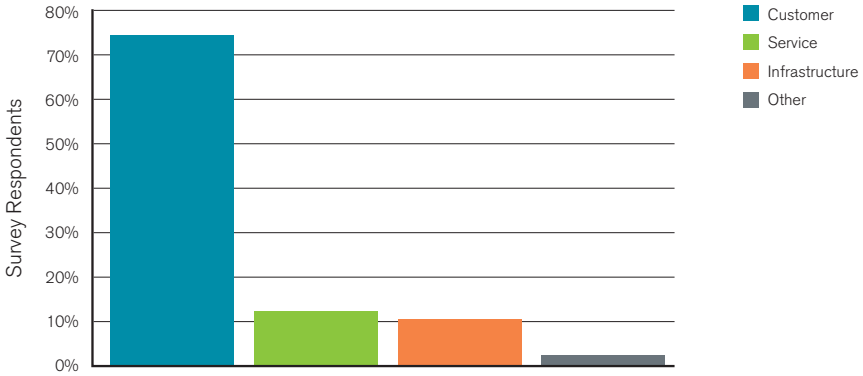

Figure 16 *Source: Arbor Networks, Inc.*

Several respondents shared details of the highest-bandwidth attacks they've observed during the survey period:

- "We were a primary target of the WikiLeaks/Anonymous incident, experiencing ~100 attacks over 10 days and covering more or less the full gamut of DDoS attack types. Unrelated 6.5 Gbps attack was IP fragments, 1500-byte packets, highly distributed."
- "DDoS against UDP/80, 29 Mpps. Do I need to say more?"
- "Slowloris-based attack linked to WikiLeaks."
- "We faced a side-effect of a spam botnet which tried to resolve nonexistent domain names, causing high loads of NXDOMAIN answers."
- "Mostly invalid packets that were stopped at our border routers via ACLs. Sources were mostly from Europe, target was a Russian Webcam recruitment site. The observed size of the attack was 30 Gbps, but the overall attack was larger than 50 Gbps and hitting capacity restraints within our providers' networks."
- "Attackers leveraging large amounts of insecure game servers to carry out multi-gigabit reflection/amplification attacks."
- "Flood of UDP traffic to an unused IP address within our mobile data network."
- "4.4 Mpps attack was an attack using malformed DNS queries toward our DNS resolvers—payloads included either a bunch of NULL characters or the string '0123456789ABCDE.' Unknown which of our customers the attack was aimed at or what the motive was. 3.4 Gbps attack was a DNS reflection/amplification attack against our DNS infrastructure in which the attacker sent ANY–record queries for isc.org to approximately 3,300 recursive DNS servers, mainly in the U.S."

- "Not sure of the initial exploitation vector (possibly several), but a large number of compromised US-based Web servers had a Perl script uploaded into /tmp and executed several times over several months. This script caused the servers to send out large volumes of UDP packets to the targeted host. There was ramp-up from 200 Mbps up to 12 Gbps as we applied reverse proxy services on a variety of networks. Attack volume was scaled up over a 3-month period to always slightly exceed our capacity, and the timings of that scaling seemed to indicate a human was doing this deliberately in response to our defensive moves. After we handled 12 Gbps successfully for about 6 hours, the attacks stopped 'permanently'—it has now been 6 months since that last attack of this type. Some of the big US hosts that were running the attackers' Perl script were sending upwards of 500 Mbps individually, and it was difficult (read: impossible) to contact their owners to have them stop it (in many cases it seemed they didn't even notice it) in a timely manner. So, with that said, the number of attacking hosts wasn't the problem—a small number of very large, high-bandwidth attacking hosts was the main issue (I'd say less than 20 single hosts accounted for 6-8 Gbps of the attack!). Traffic was not spoofed and was the legitimate source as all web hosts who did end up responding to us found the script leftover in /tmp, or running at the time they investigated."
- "Motivation: take down a games Web site. Methodology: pure, old-fashioned bandwidth-based attack."
- "Attack against a Web server—many unanswered requests which hit the firewall, taking it down."
- "There was 1.2 Gbps attack towards single host. Varied packet size—mostly 1500-byte packets and quite a lot of 64-byte packets to bring down the processing power of the customer access router."
- "Automated system made malformed HTTP requests. It moved with the DNS, but couldn't handle HTTP/S, so we moved the site to HTTP/S-only for a month. No motivation understood or known—wasn't even a major site of ours. Possibly a miscreant used the target IP address in a PTR-record entry previously, and an angry criminal rival attacked, thinking it was still in use by the original miscreant?"
- "SYN-flood which peaked an inbound interface, and was measured at ~14 Mpps."
- "UDP flood towards an online auction site."
- "Packet-based flood, motivation was immature—site was a community Web forum."
- "The largest DDoS attacks we've seen have been focused on our email infrastructure—i.e., POP3/SMTP. Not so much large amounts of data, just thousands of individual connections."

As shown in Figure 17, nearly 47 percent of respondents indicated that they experienced 1 to 10 DDoS attacks per month during the survey period, while over 44 percent experienced 10 to 500 or more DDoS attacks per month.

Average Number of DDoS Attacks per Month

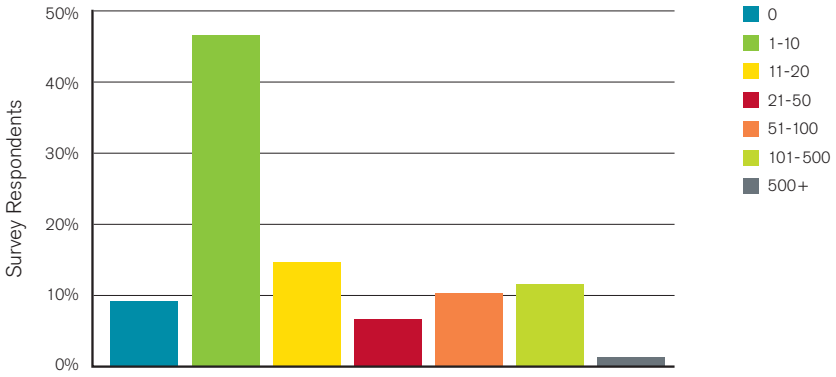

Figure 17 *Source: Arbor Networks, Inc.*

As illustrated in Figure18, commercial flow-telemetry collection/analysis systems, such as Arbor's Peakflow® SP solution ("Peakflow SP"), were the leading tools used to detect and classify the highest-bandwidth attacks experienced by respondents during the survey period. Custom in-house developed tools and various other mechanisms were the second- and third-most popular solutions in this category, respectively.

Tools Used to Measure Highest-Bandwidth DDoS Attacks

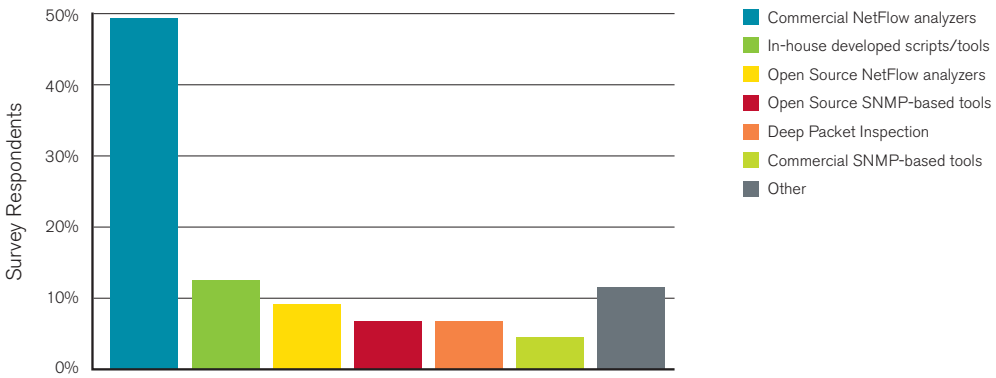

Figure 18 *Source: Arbor Networks, Inc.*

While the prevalence of complex multi-vector DDoS attacks has steadily increased over the last several years, Figure 19 indicates that nearly 27 percent of survey respondents have experienced multi-vector DDoS attacks involving both flood-based and application-layer components during the last 12 months. This represents a significant escalation on the part of attackers and is consistent with their increased usage of application-layer attack methodologies.

Multi-Vector DDoS Attacks

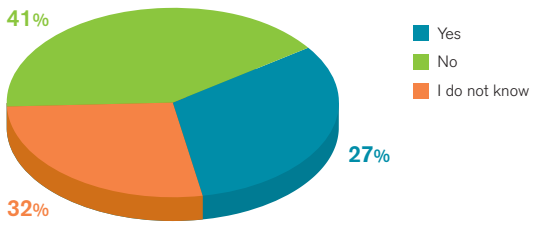

Figure 19 *Source: Arbor Networks, Inc.*

During the last 12 months, our experiences in working with network operators worldwide in mitigating DDoS attacks seemingly coincided with an apparent increase in the prevalence of ideologically-motivated "hacktivist" DDoS attacks. While we noted this trend, it was our belief that this was merely indicative of our subjective experiences and those of our customers, combined with generally heightened awareness of ideologically-motivated DDoS attacks following the well-publicized WikiLeaks/Anonymous series of incidents.

When we made the decision to query this year's survey respondents regarding their assessment of DDoS attack motivations, we expected "Unknown" to constitute the overwhelming majority of responses, with nihilism/vandalism, DDoS-enabled extortion and inter-criminal disputes making up most of the remainder.

Therefore, the results in Figure 20—which indicate that ideology or "hacktivism" ranks as the single most commonly observed motivation for DDoS attacks, with online gaming-related attacks ranked second—were surprising, while at the same time confirming our subjective observations during the survey period.

Attack Motivations Considered Common or Very Common

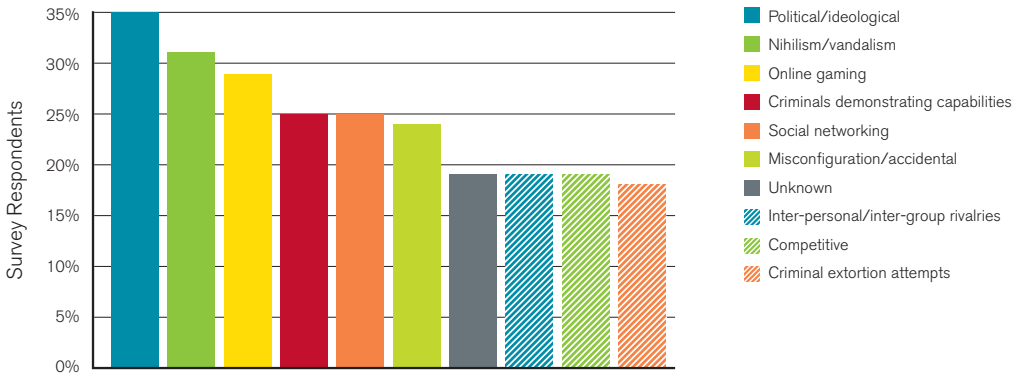

Figure 20 *Source: Arbor Networks, Inc.*

We believe this finding may well comprise one of the single most important data points in this year's report, with major implications in terms of threat assessment, situational awareness and continuity of operations for network operators, governmental bodies, law enforcement agencies and end customers alike.

Some additional free-form comments in response to this question follow:

- "As a network operator, we see the traffic, but seldom are privy to the motivation behind the attack. I think that in many cases, our customers (colleges and universities) don't know why the attack happened either—they just deal with it."
- "[We see] attacks against online auction sites which are similar to attacks against online gaming sites and attacks intended to manipulate financial markets."
- "We've experienced Quake 3/Source Engine-based exploit attacks. Attackers are abusing legitimate game servers to send specially-crafted attack packets directing them to attack others, similar to DNS reflection/amplification attacks."

In this year's survey, we asked respondents about the longest-duration DDoS attack they had observed during the survey period. Responses varied widely, ranging from "a few minutes" to "six months, with bursts and calm stages."

We also asked respondents about the average cost to their organizations of handling a DDoS attack. Several free-form responses follow:

- "Approximately $250,000 USD/incident."
- "$8,000 USD/incident."
- "Approximately 1,000EUR/incident."
- "Roughly $1M USD to $1.5M USD/incident."
- "$300,000 USD/incident."
- "$1M USD/incident."
- "More than $100,000 USD/month."
- "Net revenue-generator—we offer commercial DDoS mitigation services."

In another significant development, Figure 21 reflects what we believe to be the first documented occurrences of IPv6 DDoS attacks on production Internet networks.

Experienced IPv6 DDoS Attacks

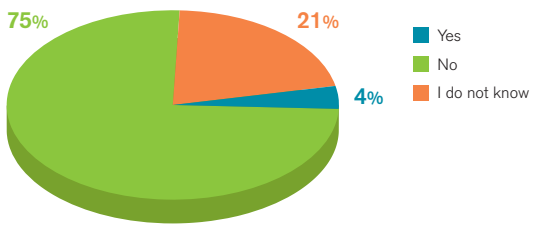

Figure 21 *Source: Arbor Networks, Inc.*

This is a significant milestone in the arms race between attackers and defenders. We believe that the scope and prevalence of IPv6 DDoS attacks will gradually increase over time as IPv6 is more widely deployed. It is also important to note that more than 75 percent of respondents do not have sufficient visibility into IPv6 traffic on their networks to detect and classify IPv6 DDoS attacks.

At the same time, the small number of reported IPv6 security incidents is an indication of how slowly IPv6 deployment and market penetration are progressing. There is a strong correlation between the economic significance of a given technology and criminal activity taking advantage of said technology. In the assessment of the Internet criminal underground, it is apparent that IPv6-enabled Internet properties simply are not yet worth the time and effort required to attack them with any frequency.

When asked why he robbed banks, career criminal Willie Sutton famously replied, "Because that's where the money is." One can draw a strong analogy between this and the way that modern Internet miscreants think. They attack where the money is.

Figure 22 indicates that over 57 percent of respondents detected and classified outbound/crossbound DDoS attacks during the survey period, a 16 percent decrease from last year's tally. Only 34 percent mitigated these attacks (Figure 23). We believe that this mitigation deficit is due in part to an almost exclusive focus on technical means for mitigating inbound attacks, along with some level of misperception that outbound/crossbound attacks are somehow less serious from an operational point of view.

Detection of Outbound/Crossbound DDoS Attacks

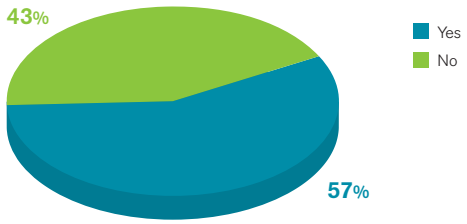

Figure 22 *Source: Arbor Networks, Inc.*

Mitigation of Outbound/Crossbound DDoS Attacks

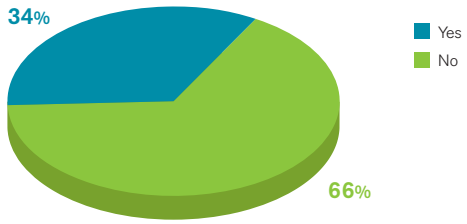

Figure 23 *Source: Arbor Networks, Inc.*

Outbound/crossbound DDoS attacks consume end-customer and operator bandwidth and often affect ancillary operator services such as DNS. This adversely affects peering ratios and results in increased transit costs. These attacks can also lead to SLA and billing disputes with end customers. Therefore, outbound/crossbound DDoS attacks warrant the same mitigation actions as inbound attacks as a matter of self-preservation.

Attack Detection, Classification and Traceback

The composition of tools used to detect, classify and traceback DDoS attacks (Figure 24) generally corresponds to responses noted in the section of this report entitled "Scale, Targeting and Frequency of Attacks" (page 15).

Use of Network Traffic Detection/Classification Tools

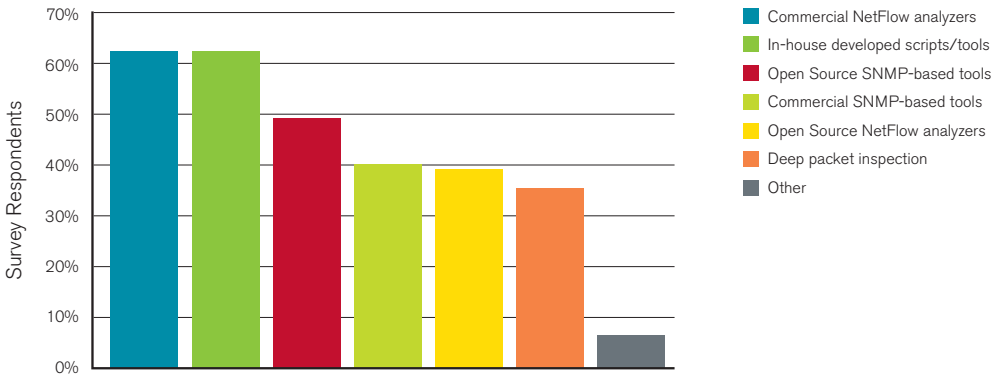

Figure 24 *Source: Arbor Networks, Inc.*

This section identifies the tools used to detect and classify the single-largest DDoS attack experienced by respondents during the survey period (Figure 25). Again, commercial flow-telemetry collection/analysis systems were by far the most commonly used tool. More day-to-day emphasis has been placed by operators on in-house developed tools, open source NetFlow analyzers, open source SNMP-based tools and deep packet inspection over commercial SNMP-based tools.

Tools Used to Measure Highest-Bandwidth DDoS Attacks

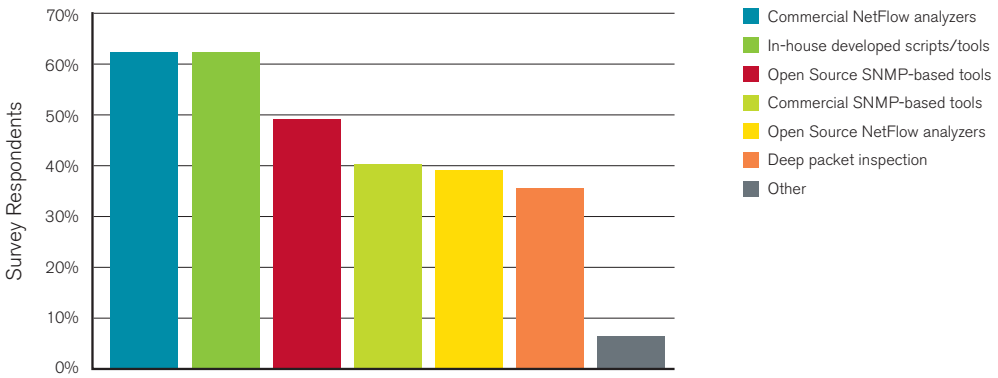

Figure 25 *Source: Arbor Networks, Inc.*

Other tools reported in use by respondents include IDS, syslog-based analysis systems, sinkholes, darknets, honeypots and NMS.

Figure 26 illustrates that while over 41 percent of respondents indicate they do not employ event-correlation tools to assist in detecting and classifying DDoS attacks, nearly 59 percent make use of either commercial, in-house developed or open-source correlation systems.

Deployment of Event-Correlation Systems

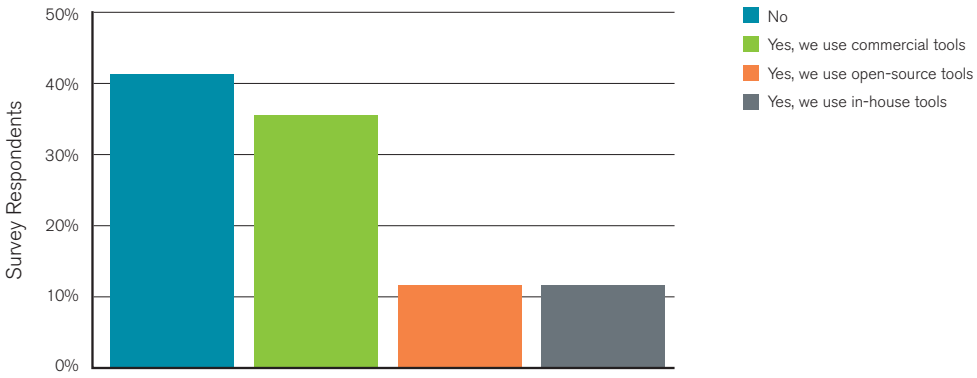

Figure 26 *Source: Arbor Networks, Inc.*

Attack Mitigation Techniques and Average Time to Mitigate

As in previous reports, despite their functional and operational limitations, ACLs continue to be the single most widely used tool to mitigate DDoS attacks (Figure 27). Destination-based, remotely-triggered blackholes (D/RTBH) and intelligent DDoS mitigation systems (IDMS) such as the Peakflow® SP Threat Management System ("TMS") and the now-discontinued Cisco Guard are the second and third most widely used mitigation mechanisms, respectively.

DDoS Mitigation Tools Used

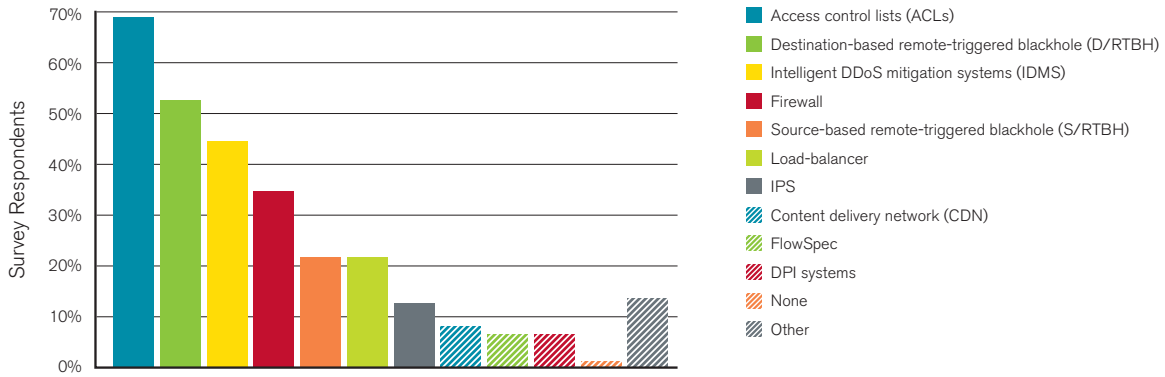

Figure 27 *Source: Arbor Networks, Inc.*

Approximately 53 percent of respondents indicated that D/RTBH is still in common use—despite the fact that D/RTBH blocks all traffic to the target and essentially completes the DDoS attack for the attacker, penalizing the victim. Other techniques utilized by respondents include custom-coded application-layer classification tools, CDNs, DPI systems, load-balancers and GeoIP-based blocking of attack traffic purportedly emanating from specific geopolitical localities.

Once again this year, no respondents indicated that QoS is still in general use as an attack mitigation technique for inbound DDoS attacks. Rate-limiting inbound traffic to attack targets invariably has the unintended side effect of enabling attack traffic to "crowd out" traffic from legitimate sources.

Nearly 47 percent of respondents indicated that they are able to successfully mitigate DDoS attacks within 20 minutes (Figure 28), a slight decrease from last year. Nearly 33 percent indicated mitigation times in excess of 30 minutes, more than double the number of operators reporting longer mitigation times than last year. This may be a result of the increasing popularity of complex application attacks that are often more difficult to detect and mitigate.

Average Time Required to Mitigate DDoS Attacks

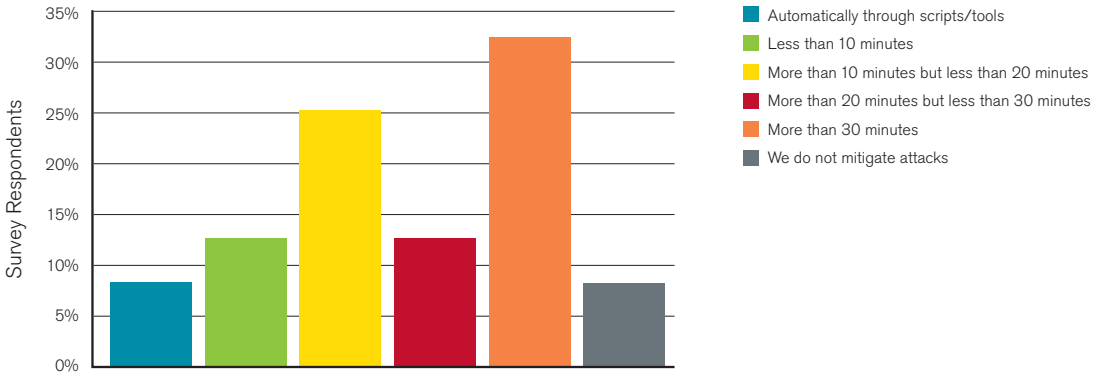

Figure 28 *Source: Arbor Networks, Inc.*

Focusing specifically on outbound/crossbound DDoS attacks (Figure 29), ACLs once again are the single most widely utilized tool to mitigate attack traffic. Over 29 percent of respondents indicated that firewalls were used to mitigate outbound/crossbound attacks, raising the specter of firewall state-table depletion as a possible DDoS vector. Meanwhile, nearly 28 percent indicated that they do not mitigate outbound/crossbound attacks at all.

Tools Used to Mitigate Outbound/Crossbound DDoS Attacks

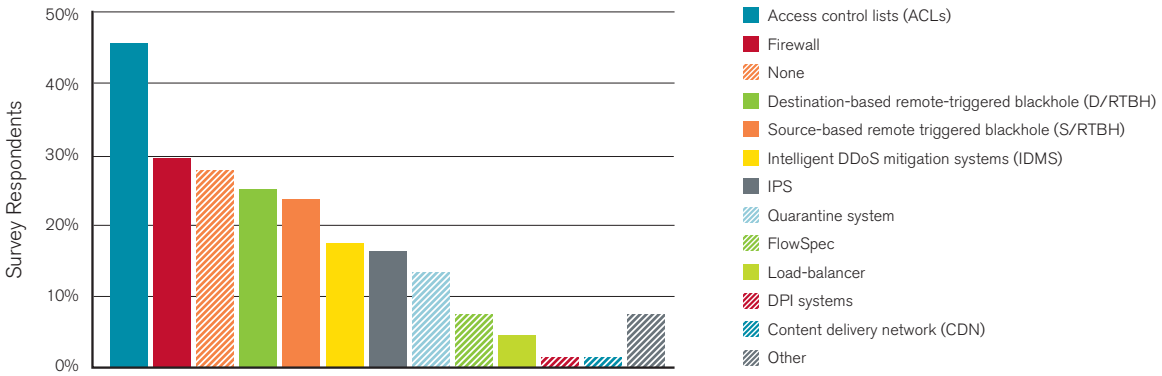

Figure 29 *Source: Arbor Networks, Inc.*

Other tools and techniques utilized to mitigate outbound/crossbound DDoS attacks include D/RTBH, S/RTBH, IDMS, IPS, FlowSpec and in-house-developed quarantine systems.

The overwhelming majority of respondents indicated that they do not proactively block known botnet C&C servers, malware drop servers and phishing servers at this time (Figure 30). Nearly 24 percent indicated that they do in fact attempt to block these undesirable hosts on a proactive basis.

Proactive Blocking of Botnet C&Cs, Malware Drop Sites and Phishing Servers

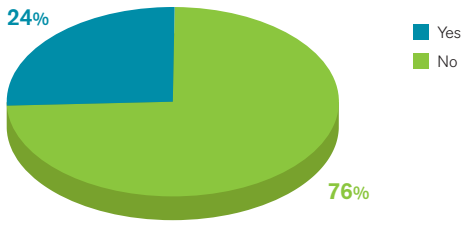

Figure 30 *Source: Arbor Networks, Inc.*

Managed Security Services

Forty-five percent of respondents indicated that they offer managed security services (Figure 31), with the most popular being managed router, managed VPN and CPE firewalls (Figure 32). Of this pool of respondents, more than 58 percent offer Clean Pipes managed DDoS mitigation services, a slight increase over last year.

Offer Managed Security Services

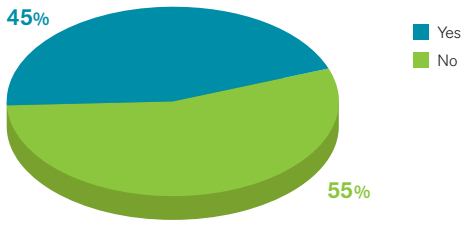

Figure 31 *Source: Arbor Networks, Inc.*

Type of Managed Security Services Offered

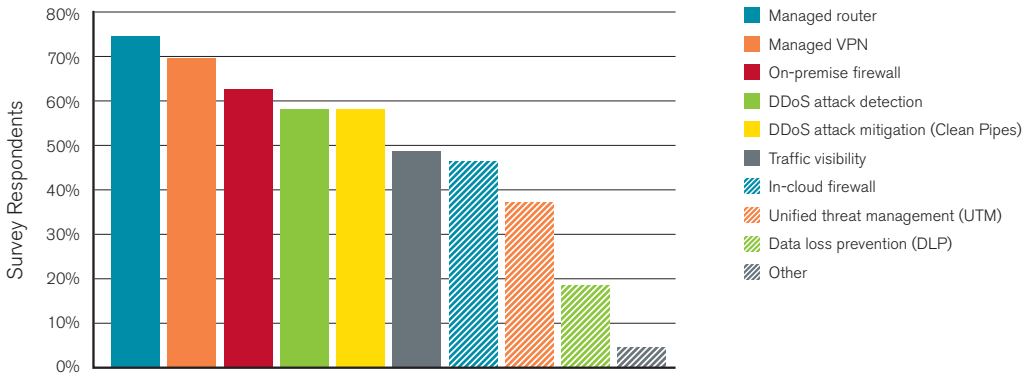

Figure 32 *Source: Arbor Networks, Inc.*

Of the respondents offering Clean Pipes managed DDoS mitigation services, 54 percent offer end customers the option of self-initiating DDoS mitigation (Figure 33), a significant increase over previous reports. This year-over-year continuity in the availability of self-mitigation options indicates that network operators view Clean Pipes as a mature service and that end customers may safely be provided with the ability to mitigate incoming DDoS attacks upon demand.

Self-Initiated DDoS Mitigation for Clean Pipes Customers

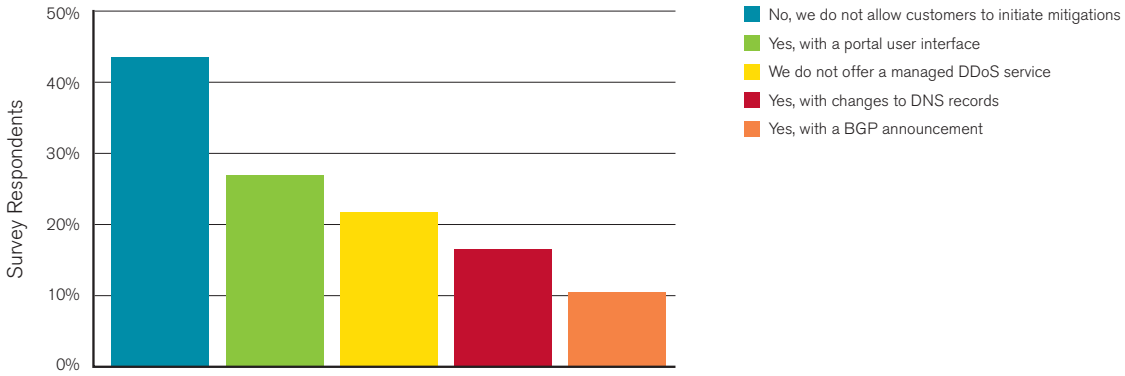

Figure 33 *Source: Arbor Networks, Inc.*

Respondents offering managed security services reported a small head count of dedicated managed security services personnel, with nearly 28 percent employing more than 10 dedicated staff members (Figure 34), an 11 percent increase year over year.

Managed Security Service Head Count

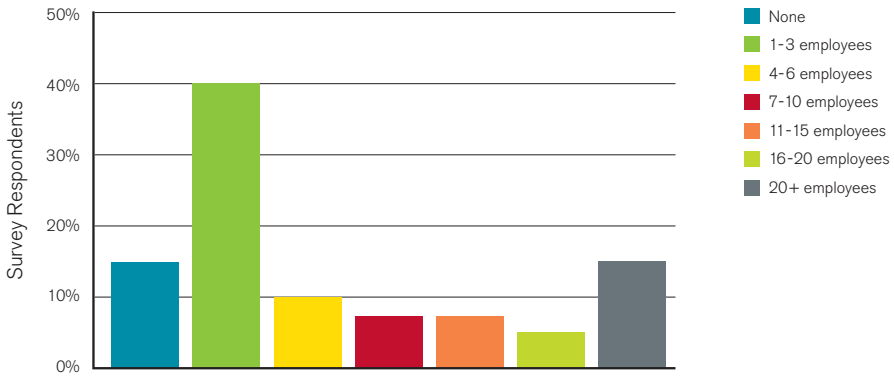

Figure 34 *Source: Arbor Networks, Inc.*

Observations on OPSEC Groups, Law Enforcement, CERTs and CSIRTs

Figure 35 identifies the numbers of network engineering personnel, network operations personnel and dedicated OPSEC personnel employed by respondents. The majority of respondents employ 10 or fewer dedicated OPSEC staff members.

OPSEC Team Head Count

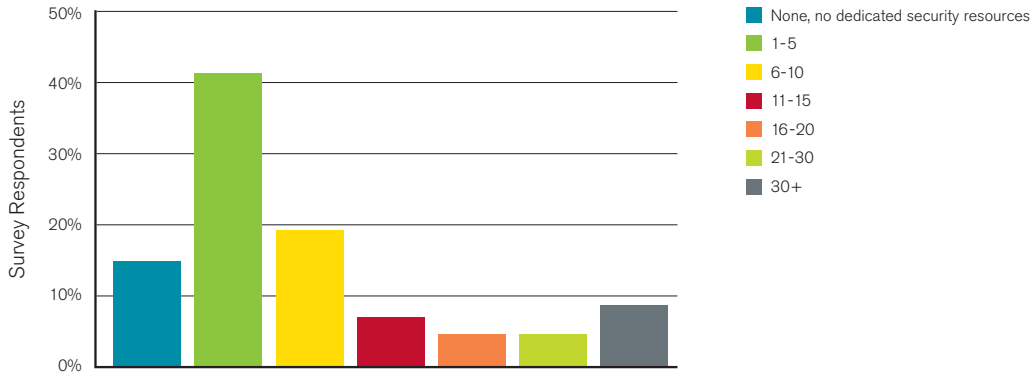

Figure 35 *Source: Arbor Networks, Inc.*

As in previous reports, lack of head count and/or resources topped the list of operational security challenges faced by respondents (Figure 36). Other significant challenges reported by this year's respondents include the difficulty of finding and retaining skilled personnel, lack of management support, lack of stakeholder support and CAPEX/OPEX funding. Free-form responses to this question included the following:

- "Customers do not want to pay for it."
- "Size of organization insufficient to warrant a dedicated team."
- "Cost of good people."
- "Lack of awareness on the part of managers and business decision-makers. In our region, many organizations are just starting to become cognizant of information security risks."

Systemic OPSEC Team Challenges

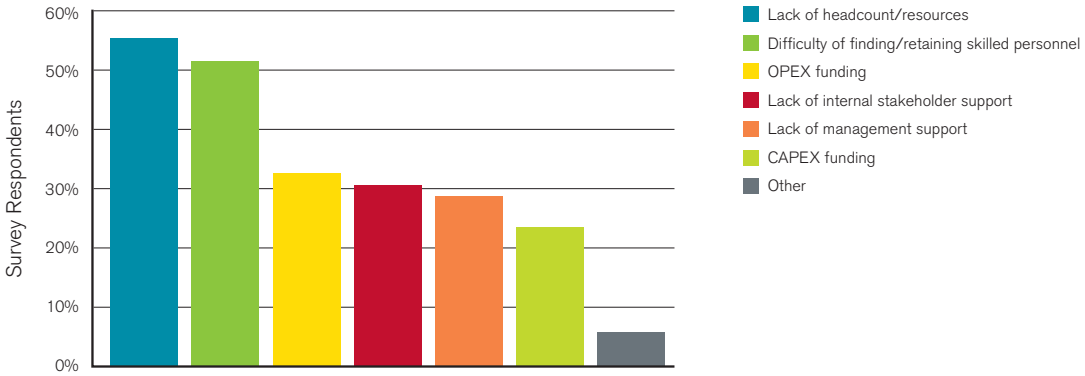

Figure 36 *Source: Arbor Networks, Inc.*

Figures 37 and 38 illustrate that approximately 90 percent of respondent organizations operate a NOC, and only 46 percent operate a SOC—the latter representing a 9 percent increase year over year.

NOC Presence by Organization

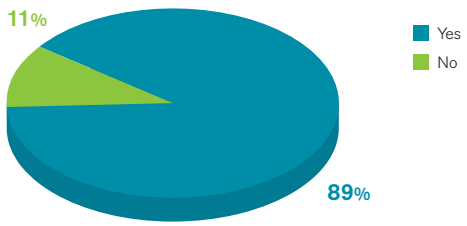

Figure 37 *Source: Arbor Networks, Inc.*

SOC Presence by Organization

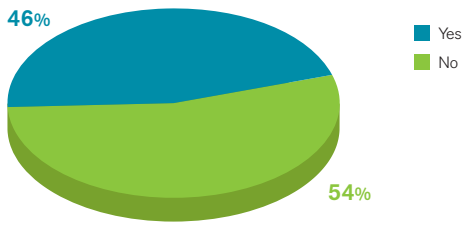

Figure 38 *Source: Arbor Networks, Inc.*

OPSEC teams response readiness saw a marked improvement over last year. Over 58 percent of respondent organizations never rehearse their operational security plans and procedures or conduct OPSEC drills (Figure 39), while in the last survey, 72 percent of respondents indicated that they did not exercise their plans. We believe this 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 comment from this section follows:

- "We don't practice, but we do have basic plans that we would implement. We also maintain close relationships with external upstream network providers for rapid escalation of problems."

Frequency of DDoS Defense Rehearsals/Drills

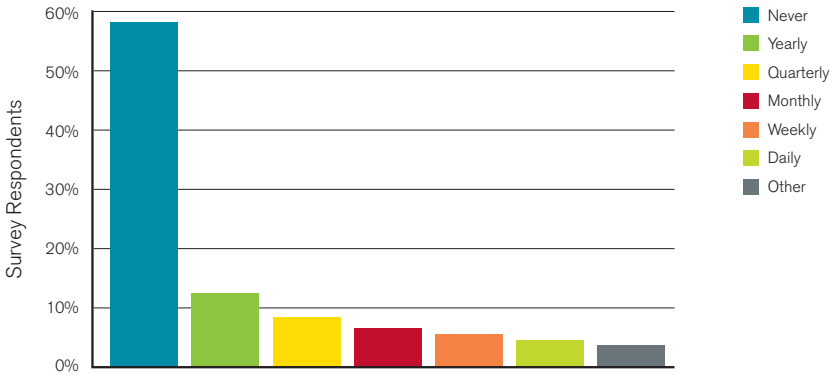

Figure 39 *Source: Arbor Networks, Inc.*

Nearly 81 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 40).

Although this seems like a very basic requirement for any Internet-connected organization, we continue to observe numerous instances in which outage-inducing DDoS attacks are unnecessarily prolonged due to the lack of this basic contact information by the relevant parties.

Maintain Current Contact Information for Peers/Transits/Customers/OPSEC Teams

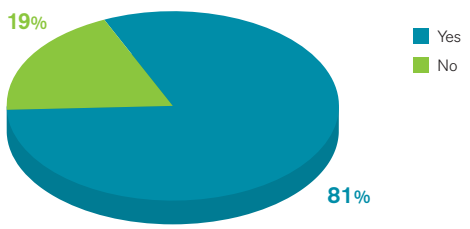

Figure 40 *Source: Arbor Networks, Inc.*

Security-related email lists remain the single most popular way of staying aware of relevant security information from outside sources (Figure 41). Other popular methods reported by this year's respondents include industry conferences, vendor-specific email lists and blogs, and social networking systems such as Twitter, Facebook, etc.

Other primary sources of security-related information utilized by respondents include closed and vetted operational security groups, FIRST, and various CERT and CSIRT organizations. These responses are in line with findings from last year's report.

External Sources of Operationally Relevant Security Information

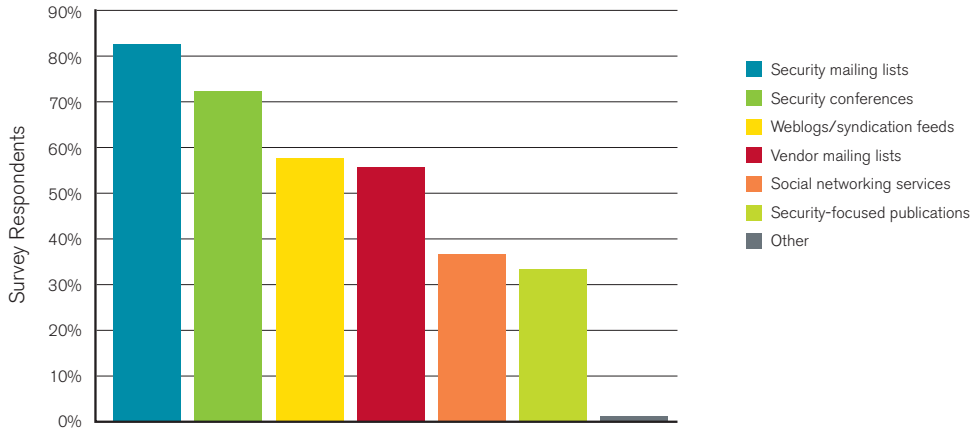

Figure 41 *Source: Arbor Networks, Inc.*

Forty-one percent of respondents indicated that they participate in closed or vetted global operational security groups (Figure 42), while nearly 87 percent indicated that they believe these groups are highly effective in handling operational security issues on an inter-organizational basis (Figure 43).

Participation in Vetted OPSEC Groups/Systems

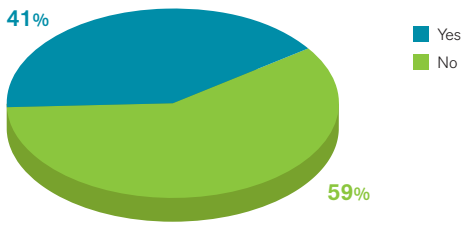

Figure 42 *Source: Arbor Networks, Inc.*

Efficacy of Global OPSEC Communities

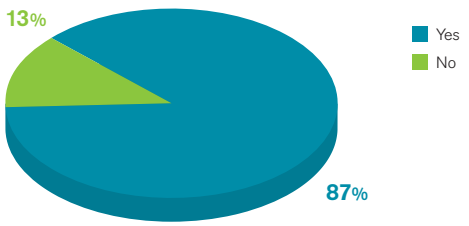

Figure 43 *Source: Arbor Networks, Inc.*

As with OPSEC teams in general, significant systemic challenges to full participation in closed/vetted global OPSEC groups persist (Figure 44). Lack of time/resources is the most frequently cited challenge, along with lack of management support, policy barriers, unclear benefits and legal concerns.

Systemic Challenges to Participation in Vetted OPSEC Groups/Systems

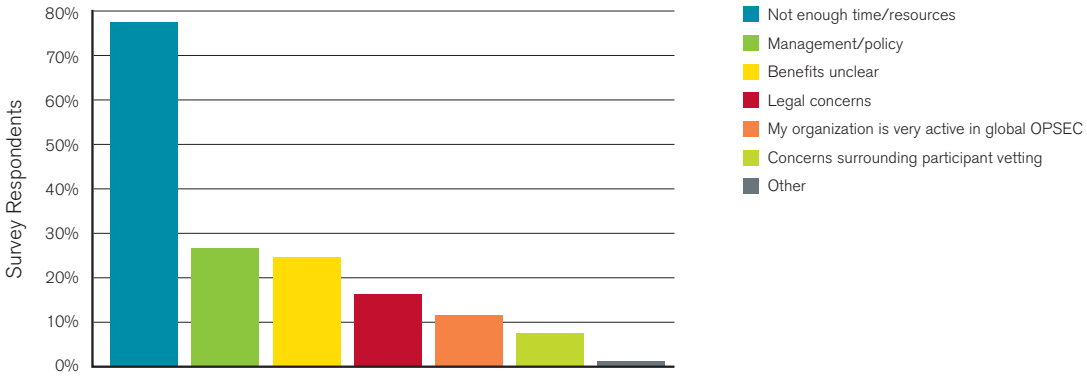

Figure 44 *Source: Arbor Networks, Inc.*

Nearly 74 percent of respondents indicated that they do not refer security incidents to law enforcement (Figure 45), a marked increase from last year. This is due to a variety of reasons, including lack of resources and time, low confidence in law enforcement investigative efficacy and corporate policy (Figure 46). Some free-form comments from respondents who do not currently make law enforcement referrals follow:

- "Attacks we see are sourced from foreign jurisdictions."
- "Responsibility and decision rest with our customers."

Attacks/Incidents Referred to Law Enforcement

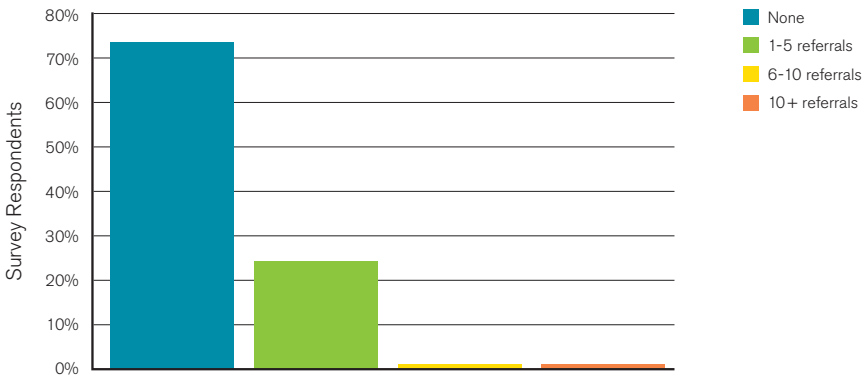

Figure 45 *Source: Arbor Networks, Inc.*

Systemic Challenges in Law Enforcement Referrals

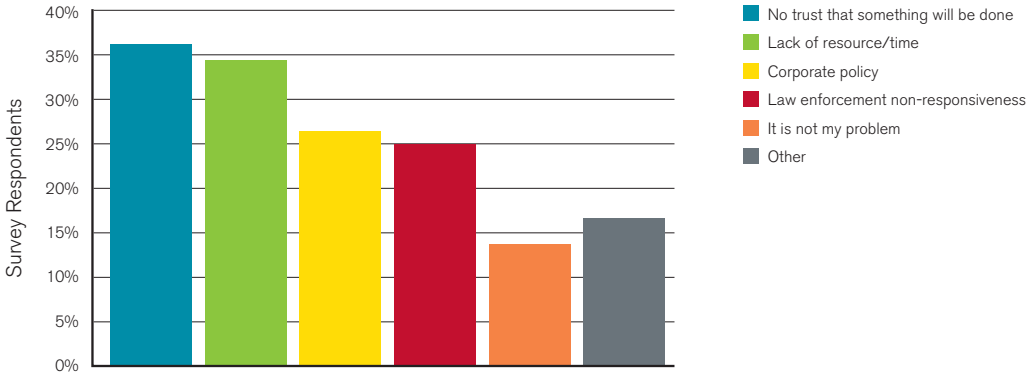

Figure 46 *Source: Arbor Networks, Inc.*

Overall, confidence in law enforcement efficacy is quite low (Figure 47). However, a plurality of respondents does in fact see evidence of positive change in law enforcement efficacy year over year (Figure 48).

We also note that a relatively small number of respondents have apparently forged successful and mutually beneficial relationships with their respective law enforcement agencies, and consequently made a significant number of incident referrals to those agencies during the survey period. It is our hope that this formula can be replicated elsewhere, leading to greater and more fruitful law enforcement involvement in the identification and prosecution of Internet criminals.

Confidence in Law Enforcement Investigative Efficacy

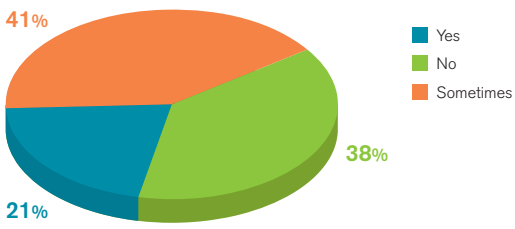

Figure 47 *Source: Arbor Networks, Inc.*

Perceived Changes in Law Enforcement Investigative Efficacy

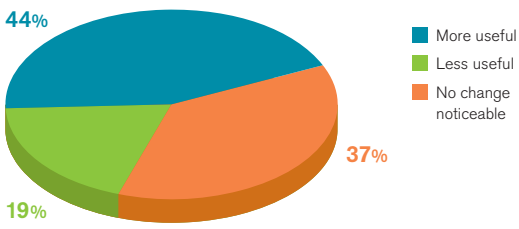

Figure 48 *Source: Arbor Networks, Inc.*

It is also our understanding that 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.

Figures 49 and 50 illustrate that over 40 percent of respondent organizations have established an internal CERT, and nearly 66 percent are actively engaged with their respective national or regional CERTs and/or CSIRTs.

Internal CERT Organization

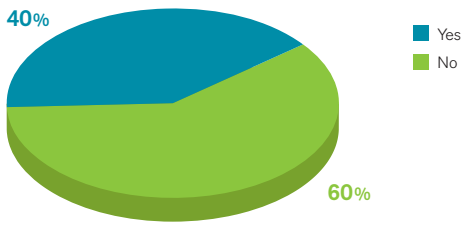

Figure 49 *Source: Arbor Networks, Inc.*

Engagement with National/Government CERT/CSIRT

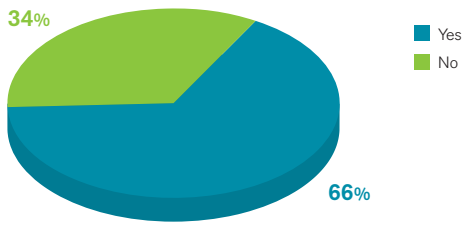

Figure 50 *Source: Arbor Networks, Inc.*

Nearly 82 percent of respondents believe that government CERTs/CSIRTs have a positive role to play in operational security incident response and welcome their involvement (Figure 51). Respondents who do not engage with national or regional CERT/CSIRT organizations cite lack of time and resources; lack of information about their national/regional CERT/CSIRT organizations; lack of management support; and, in some cases, the fact that no national/regional organization of this type exists within their respective geographies. Additionally, 73 percent of respondents are concerned that governments are not doing enough to protect critical network infrastructure (Figure 52).

Desirability of National/Government CERT/CSIRT Engagement

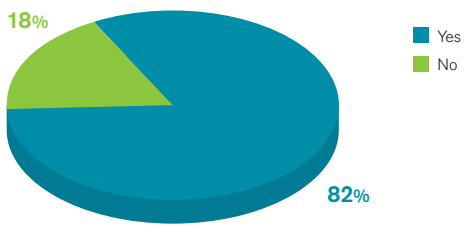

Figure 51 *Source: Arbor Networks, Inc.*

Concerned with Government Efforts for Critical Infrastructure Protection

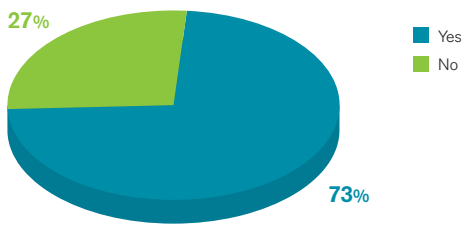

Figure 52 *Source: Arbor Networks, Inc.*

Infrastructure Protection Techniques

Figure 53 illustrates that a majority of respondent organizations have implemented best current practices (BCPs) in critical network infrastructure security, representing significant progress over last year. These BCPs include routing protocol authentication; iACLs to keep undesirable traffic away from their network infrastructure devices; and anti-spoofing measures at the edges of their networks.

A plurality 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 38 percent perform IRR registration of their customer routes.

Network Infrastructure BCPs Implemented

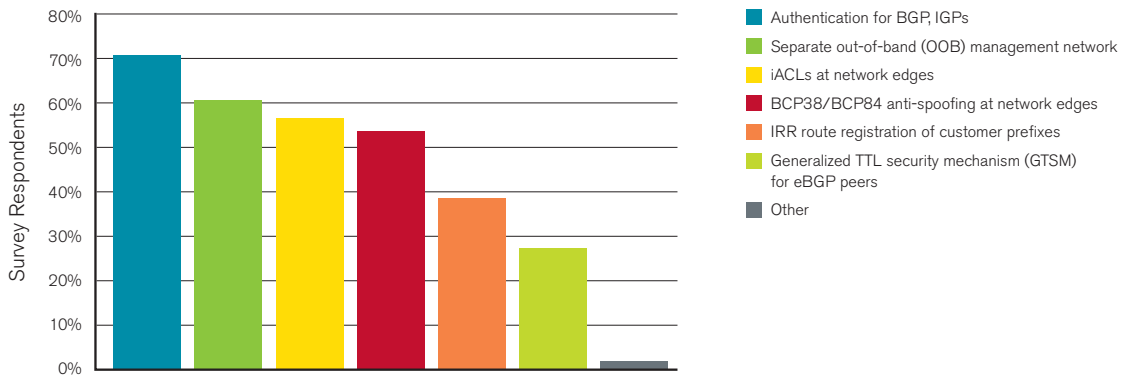

Figure 53 *Source: Arbor Networks, Inc.*

Based on survey responses, 72 percent of data center operators have implemented various Layer 2 BCPs (Figure 54). These include loop guard; root guard; BPDU guard; IP source guard/DHCP snooping (which also works with fixed IP addressing); pVLANs; VACLs; PACLs; and other useful Layer 2 infrastructure security techniques.

Similar good news exists on the route-filtering front, with 79 percent of respondent organizations explicitly filtering customer route announcements (Figure 55).

Layer 2 Infrastructure BCPs Deployed in Data Center Environments

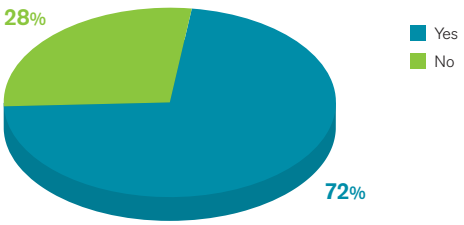

Figure 54 *Source: Arbor Networks, Inc.*

Explicit Filtering of Customer Routing Advertisements

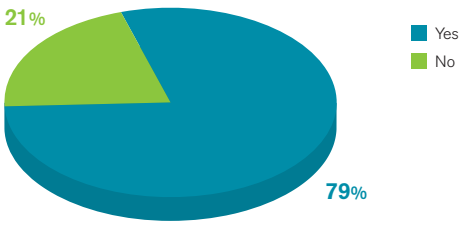

Figure 55 *Source: Arbor Networks, Inc.*

Meanwhile, only 61 percent of respondents explicitly filter inbound routing advertisements from peers and upstream transit providers (Figure 56).

Explicit Filtering of Inbound Peer/Upstream Routing Advertisements

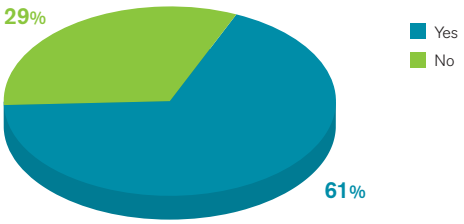

Figure 56 *Source: Arbor Networks, Inc.*

IPv6 Observations

In the 2010 *Worldwide Infrastructure Security Report,* operators indicated serious concerns regarding visibility and control parity of IPv6-enabled networks with IPv4 networks, as well as anxiety about future address allocations. These trends continue to be reflected in this year's report.

Nearly 57 percent of respondents indicated that they believe IPv4 address allocations will not prove to be a serious problem during the next 12 months (Figure 57), reflecting no change year over year. We're still unsure as to whether this continued majority view is indicative of extreme confidence in forthcoming IPv6 deployments; a sufficiency of current IPv4 address allocations that will last for some time into the future; a lack of awareness of the impending exhaustion of available IPv4 address space; or the belief that carrier-grade NAT will be sufficient in the medium term for addressing end-customer needs.

Concerns Regarding IPv4 Address Availability

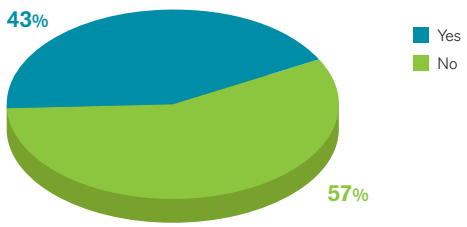

Figure 57 *Source: Arbor Networks, Inc.*

Respondents who indicated concerns regarding IPv4 address allocations and availability provided the following comments:

- "Competitors are sitting on large IPv4 allocations, and lack of industry adoption of IPv6 is problematic."
- "It's harder to get space from the RIRs, slow movement towards IPv6."
- "We are running short of IPv4 addresses and may be forced to implement NAT on a portion of our network."
- "Businesses are asking for more and more IPv4 space to hoard, and are reluctant to use IPv6."
- "Too many of our /24 CIDR blocks allocated to customers that don't actually need them; and IPv6 upgrade is very slow, due to some internal company policies."
- "Customers continuing to request large amounts of address space for non-technical reasons (bulk emailing on the rise), sales under pressure to close deals, senior management not thinking long term."
- "We extensively utilize globally unique addressing in connecting over VPNs to third parties, and are likely no longer able to justify further allocations from our RIR."

More than 74 percent of respondents stated that their production network infrastructure currently supports IPv6 today (Figure 58), representing a 10 percent increase over last year, while an additional 15 percent indicated that they plan to implement production support within the next 12 months (over 89 percent cumulative, Figure 59).

IPv6 Currently Implemented on Network Infrastructure

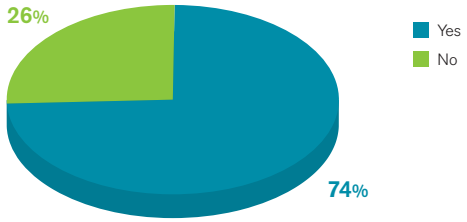

Figure 58 *Source: Arbor Networks, Inc.*

IPv6 Deployed Currently or Within Next 12 Months

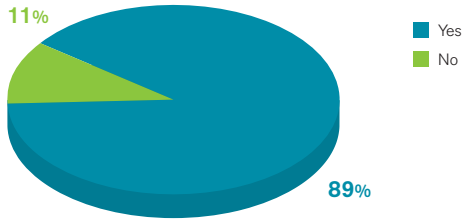

Figure 59 *Source: Arbor Networks, Inc.*

More than half of respondents indicated that they are presently making use of IPv6 on their management networks to handle interaction between their internal OSS or NMS and their network infrastructure devices such as cable modems and other commonplace elements (Figure 60). Figure 61 summarizes that over 70 percent of respondents view visibility into IPv6 traffic on their networks as critical.

IPv6 Used for Infrastructure Addressing

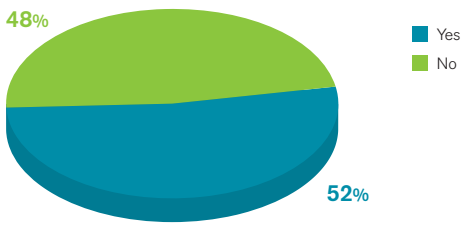

Figure 60 *Source: Arbor Networks, Inc.*

Criticality of IPv6 Network Traffic Visibility

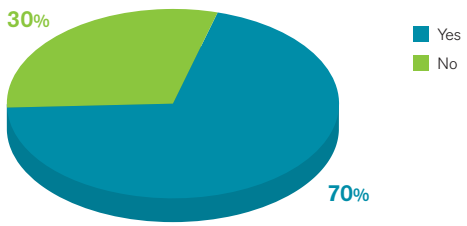

Figure 61 *Source: Arbor Networks, Inc.*

Figure 62 illustrates that more than 36 percent indicated full network infrastructure vendor support for IPv6 flow telemetry today, and nearly 27 percent indicated their current network infrastructure offers at least partial support for IPv6 flow telemetry.

Network Infrastructure Support for IPv6 Flow Telemetry

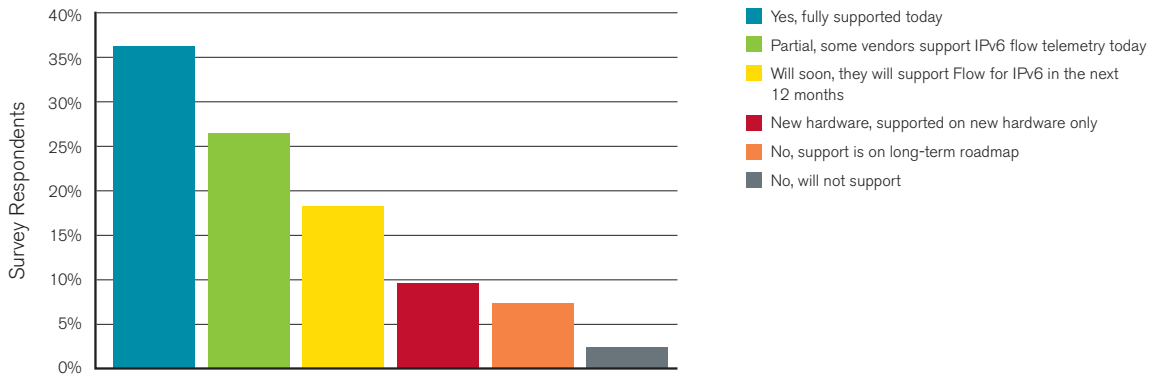

Figure 62 *Source: Arbor Networks, Inc.*

While nearly 42 percent of respondents project that their IPv6 traffic volume will increase 20 percent over the next 12 months, almost 18 percent forecast greater than a 100 percent IPv6 volume increase over the same period (Figure 63).

Anticipated IPv6 Traffic Volume Growth

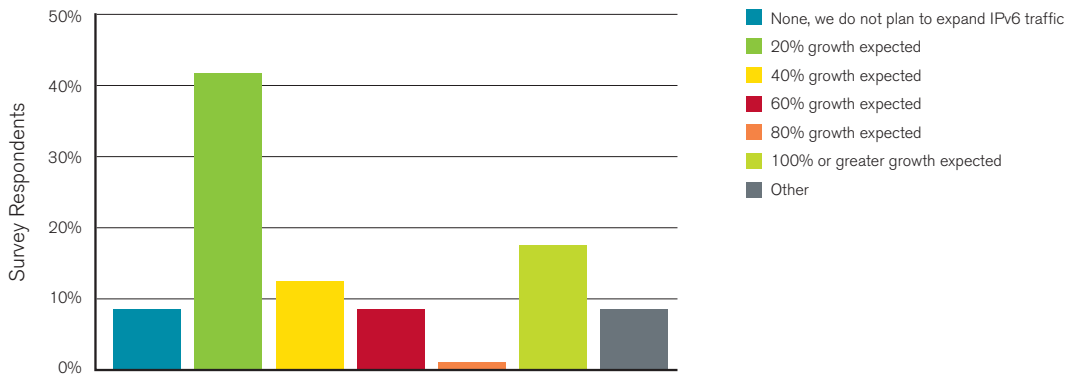

Figure 63 *Source: Arbor Networks, Inc.*

Figure 64 shows that over 65 percent of respondents stated that the lack of IPv4/IPv6 feature-parity is their foremost security concern related to IPv6. Sixty percent indicated that they have little or no visibility into their IPv6 traffic today, and thus have no ready way to detect, classify and traceback IPv6 attack traffic on their networks. Nearly 59 percent cited misconfigurations resulting in outages as a key concern. Fifty-two percent expressed concern regarding IPv6 DDoS attacks, with almost 47 percent expressing concern regarding IPv6 stack implementation flaws that may lead to security vulnerabilities in their network infrastructure elements.

IPv6 Security Concerns

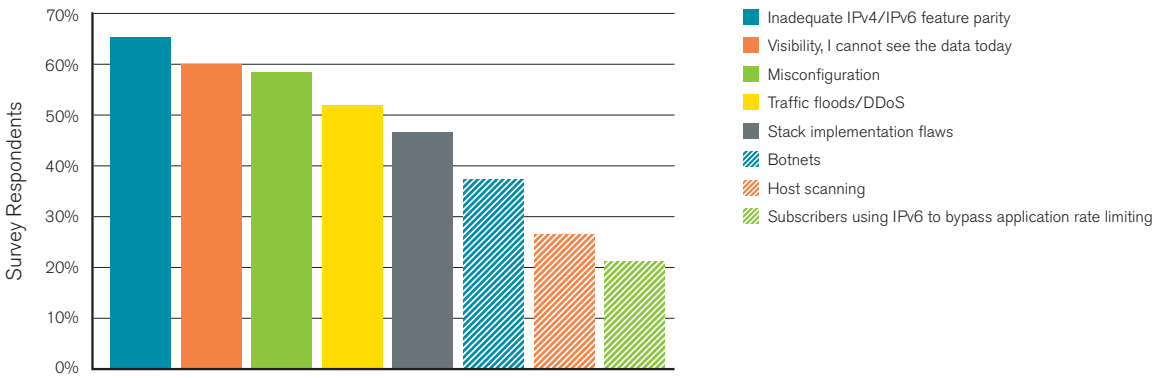

Figure 64 *Source: Arbor Networks, Inc.*

The relative lack of industry operational experience with IPv6 and the length and complexity of IPv6 addresses as compared to IPv4 addresses should motivate network operators to make use of automated provisioning systems whenever possible.

Despite the previously mentioned limitations of ACLs, nearly 63 percent of respondents reported that they use or intend to use such lists to mitigate IPv6 DDoS attacks (Figure 65). Half stated that they use or intend to use IDMS, an 11 percent increase year over year. Approximately 33 percent indicated they use or intend to use D/RTBH as an IPv6 mitigation tool, even though it has the net result of completing the DDoS on behalf of the attacker.

Current and Planned IPv6 DDoS Attack Mitigation Tools

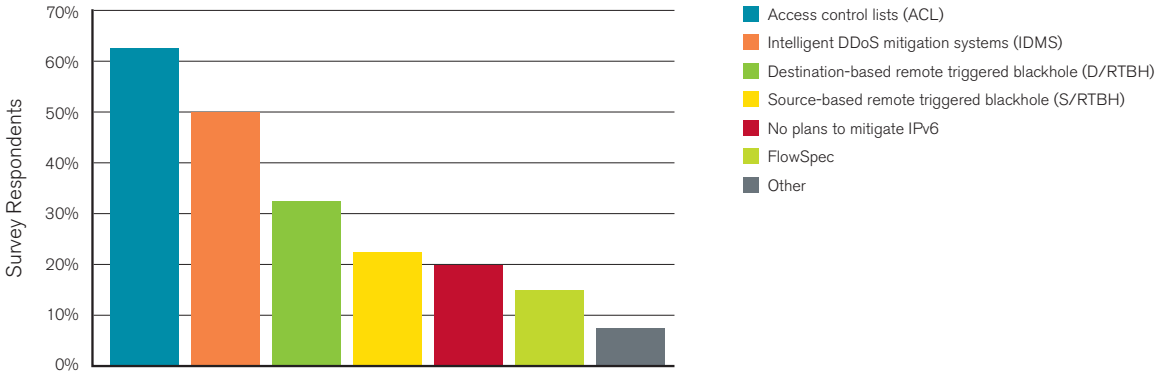

Figure 65 *Source: Arbor Networks, Inc.*

Twenty percent of respondents indicated that they have no plans to mitigate IPv6 DDoS attacks. We suspect that priorities within these organizations may evolve rapidly as IPv6 network traffic becomes more prevalent—especially given the first reports of IPv6 DDoS attacks on production networks as described earlier in this report.

It is an unavoidable consequence of IPv4 address depletion and the move to IPv6 that large amounts of undesirable state will be inserted into service provider networks in the form of 6-to-4 gateways and CGN devices. DDoS attacks are essentially attacks against capacity and/or state. The large amounts of state present in these devices make them especially vulnerable to both deliberate and inadvertent DDoS attacks.

Network operators should take this state vector for DDoS into account when incorporating 6-to-4 gateways and CGNs into their networks. We continue to recommend that operators do everything possible to minimize the amount of state concentrated in any individual device, and make use of reaction tools (such as S/RTBH) and IDMS to protect these stateful DDoS chokepoints against attack.

As more stateful 6-to-4 and CGN infrastructure devices are installed in operator networks, the risk of attacks will increase. The use of vigilance—combined with the employment of sound network infrastructure BCPs and operational security practices—can ameliorate the harmful effects of such attacks on the network.

Data Center Operator Observations

Figure 66 illustrates that more than 63 percent of respondents operate data centers. Of those respondents, over 56 percent indicated they had experienced DDoS attacks directed at targets within their data centers during the 12-month survey period (Figure 67).

Data Center Present in Network

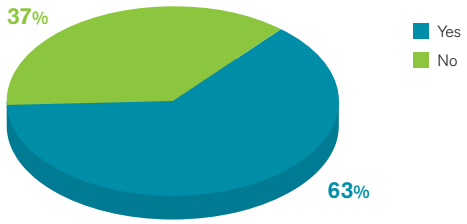

Figure 66 *Source: Arbor Networks, Inc.*

Observed DDoS Attacks Targeting Data Centers

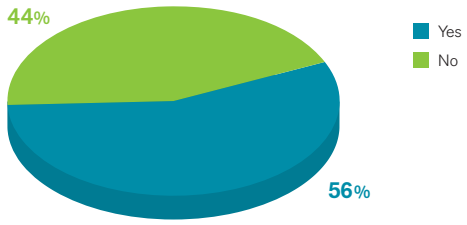

Figure 67 *Source: Arbor Networks, Inc.*

Figure 68 illustrates that 25 percent of respondents experienced a DDoS attack that exceeded the uplink capacity from their data center to their core network and/or peering/transit providers during the survey period, a 10 percent increase year over year.

However, it is important to note that lower-bandwidth, application-layer attacks can be just as effective in taking down a service or customer. This is substantiated by the high percentage of respondents who reported application-layer attacks toward services.

DDoS Attacks Exceeding Data Center Bandwidth

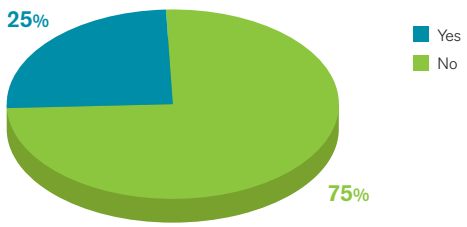

Figure 68 *Source: Arbor Networks, Inc.*

The data represented in Figure 69 emphasizes the fact that the attack surface of the data center includes the underlying services and service architecture, as well as customer properties, network-level architecture and overall capacity. Nearly 55 percent of respondents who operate data centers indicated that they experienced DDoS attacks directed at ancillary data center services such as Web portals, shared Web hosts, DNS servers and SMTP servers during the survey period.

Targets of DDoS Data Center Attacks

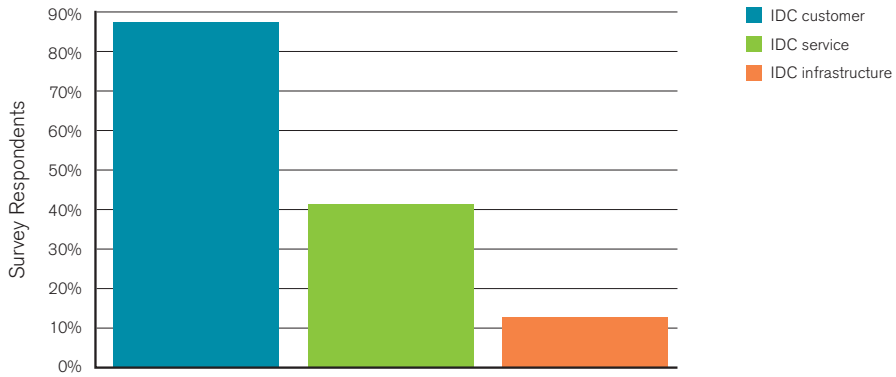

Figure 69 *Source: Arbor Networks, Inc.*

Thirty-three percent of respondents experienced more than 10 attacks per month towards their Internet Data Centers (Figure 70).

Average DDoS Attacks per Month on Data Centers

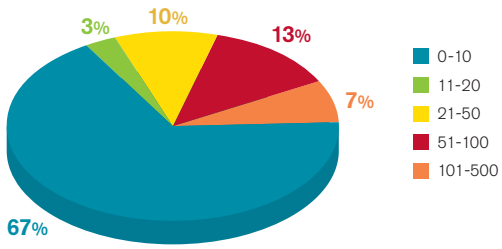

Figure 70 *Source: Arbor Networks, Inc.*

Figure 71 depicts that more than 59 percent of respondents experienced increased OPEX-related expenditures as a result of data center-targeted DDoS attacks during the survey period, while over 44 percent experienced customer churn and 37 percent reported related revenue loss due to these attacks.

Impact from Data Center DDoS Attacks

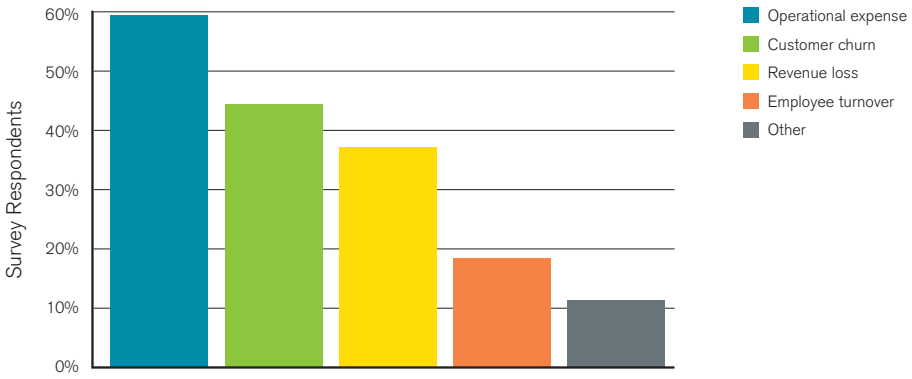

Figure 71 *Source: Arbor Networks, Inc.*

Forty-two percent of all respondents experienced stateful firewall and/or IPS failure as a direct result of DDoS attacks during the survey period (Figure 72). Only 10 percent of respondents to this set of questions indicated that they follow the data center BCP of enforcing access policy via stateless ACLs deployed on hardware-based routers/Layer 3 switches capable of handling millions of packets per second.

Failure of Stateful Firewall/IPS Due to DDoS Attacks

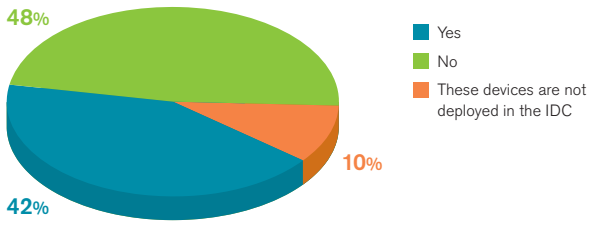

Figure 72 *Source: Arbor Networks, Inc.*

Firewall and IPS devices are stateful in-line devices and, as such, are innately vulnerable to DDoS attacks. The highest performance firewall and IPS devices available on the market are vulnerable to even moderate-size DDoS attacks that can overwhelm the state capacity of these systems. If these devices are deployed within data centers, it is strongly advisable to place them behind more robust DDoS defenses such as iACLs on hardware-based routers and dedicated IDMS devices.

The danger of unprotected stateful device failure due to DDoS attack is further highlighted by the nearly 43 percent of respondents who indicated that they had experienced load-balancer failures due to DDoS attacks during the survey period (Figure 73). As with stateful firewalls and IPS devices, if load balancers are deployed in data center networks, they must be protected by DDoS reaction/mitigation tools such as S/RTBH, FlowSpec, and/or IDMS.

Failure of Load Balancers Due to DDoS Attacks

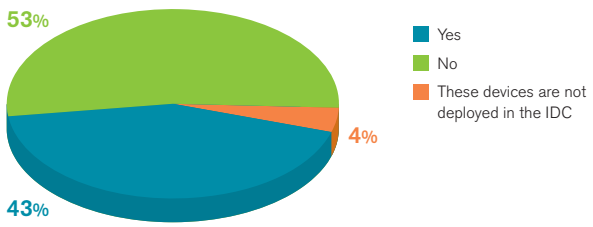

Figure 73 *Source: Arbor Networks, Inc.*

Respondents listed ACLs as a primary mechanism for mitigating DDoS attacks against data centers (Figure 74). They also identified stateful firewall and IPS devices as primary DDoS defense mechanisms. More than 62 percent of respondents indicated that they make use of IDMS to mitigate data center-targeted DDoS attacks (a 14 percent year-over-year gain), and nearly 38 percent employ S/RTBH within their data center environments, an increase of 20 percent over last year.

Primary Mechanism for DDoS Attack Mitigation

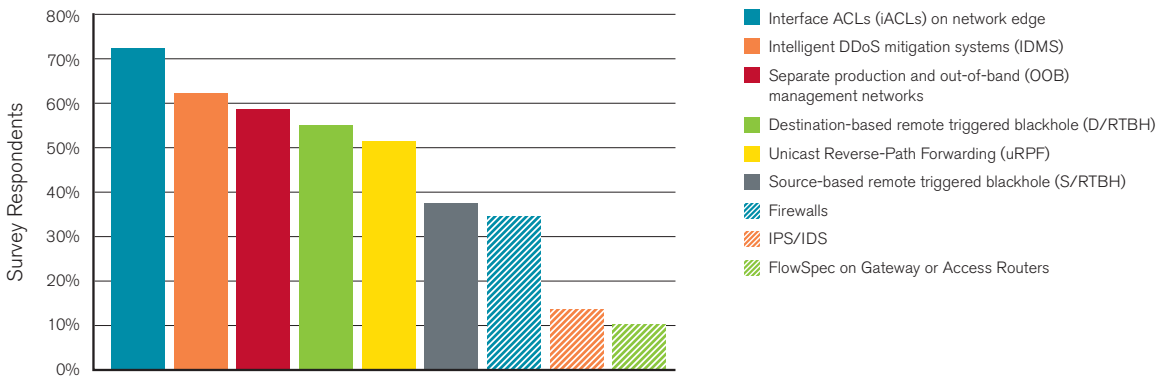

Figure 74 *Source: Arbor Networks, Inc.*

Mobile and Fixed Wireless Operator Observations

As indicated in Figures 75 and 76, nearly 27 percent of respondents operate a mobile or fixed wireless network, and in aggregate, 50 percent of those respondents serve anywhere from five million subscribers to more than 100 million subscribers on their wireless networks, a nearly identical tally with last year's responses.

Mobile/Fixed Wireless Operator

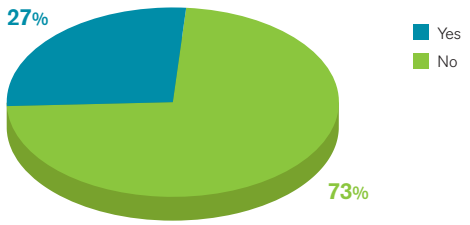

Figure 75 *Source: Arbor Networks, Inc.*

Number of Wireless Subscribers

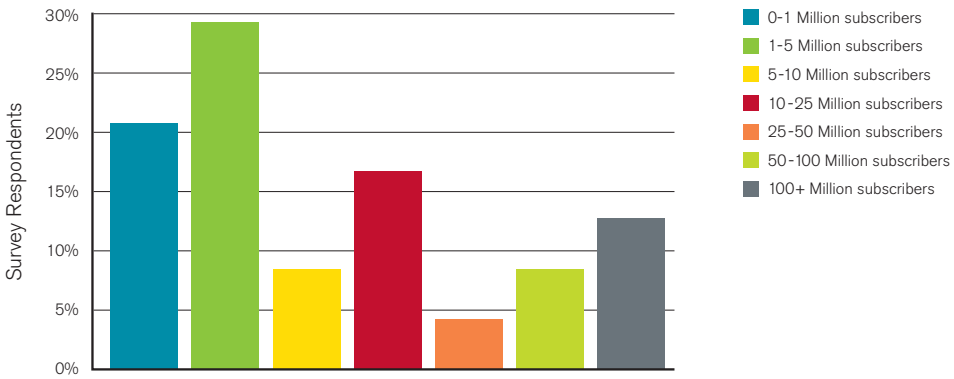

Figure 76 *Source: Arbor Networks, Inc.*

According to the data in Figure 77, over 95 percent of respondents have deployed 3G networks, approximately 5 percent operate WiMAX networks and nearly 29 percent operate LTE networks, an 18 percent year-over-year increase. The remaining respondents operate WiFi hotspot networks or self-identify as MVNOs. Figure 78 identifies that approximately 33 percent of respondents plan to deploy 4G in 2012.

Deployed Wireless Technology

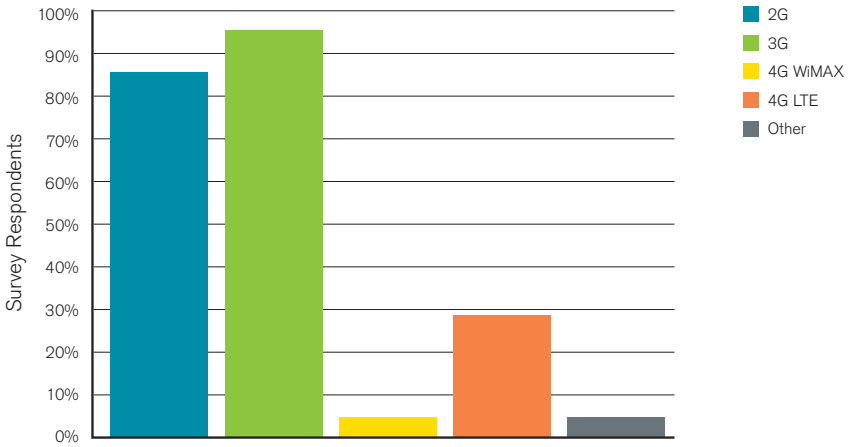

Figure 77 *Source: Arbor Networks, Inc.*

Anticipated Deployment Dates of Forthcoming 4G Networks

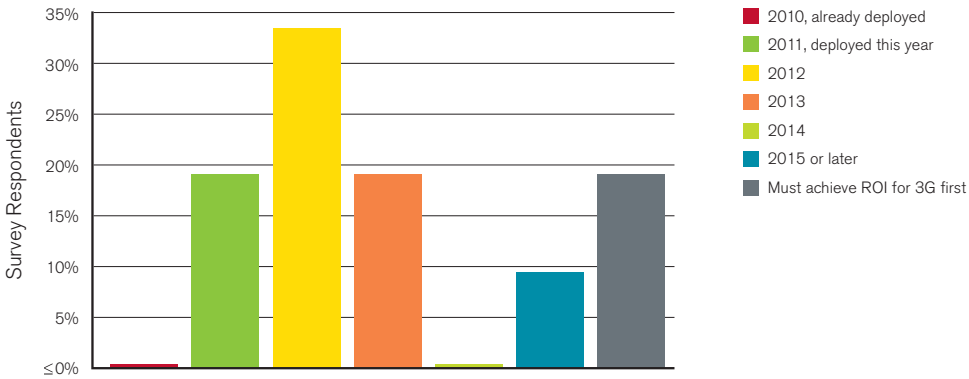

Figure 78 *Source: Arbor Networks, Inc.*

In terms of visibility into the network traffic of their wireless packet cores and their ability to classify core traffic as potentially harmful, fully 70 percent of respondents indicated that their capabilities in this area are equivalent to or better than on their wireline networks (Figure 79). Initially, we interpreted this as a significant positive change from previous reports; however, further analysis of the survey responses did not bear out this preliminary assessment. The data clearly indicates that mobile respondents have placed more of a focus on visibility than in the past and have made investments to improve in this area. However, more detailed questions further in the survey exposed significant gaps in the mobile visibility of some respondents.

Security and Visibility in Mobile Packet Core

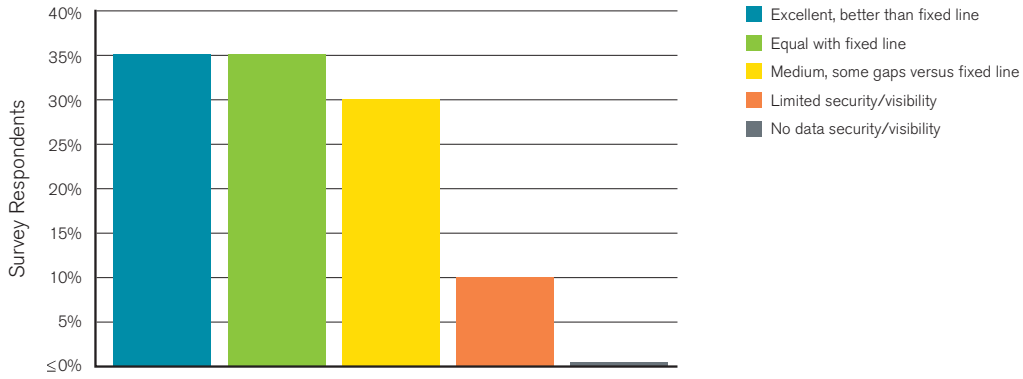

Figure 79 *Source: Arbor Networks, Inc.*

Of mobile wireless operator respondents, over 72 percent indicated that they have visibility equivalent to or better than their wireline networks at the Gi demarcation (Figure 80). Again, this is a nearly 180-degree shift from previous reports.

Security and Visibility at Mobile Gi Interface

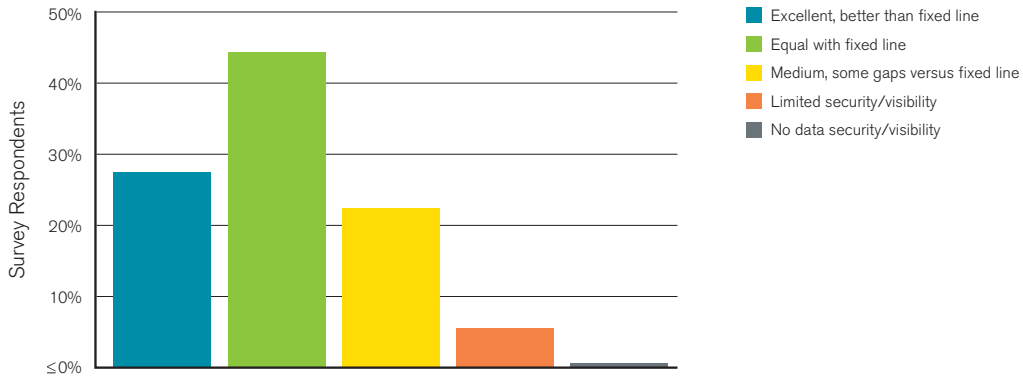

Figure 80 *Source: Arbor Networks, Inc.*

Nearly 78 percent of respondents report that they have suffered no direct attacks on their wireless-specific network infrastructure within the 12-month survey period (Figure 81). We believe this figure to be the result of significant challenges in detecting, classifying, and tracing back DDoS attacks within their network infrastructure.

Attacks Explicitly Targeting Wireless Network Infrastructure

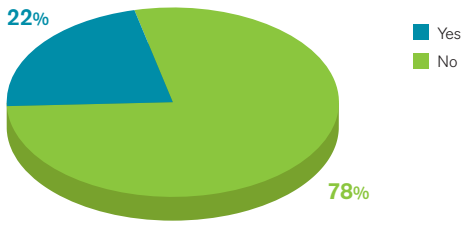

Figure 81 *Source: Arbor Networks, Inc.*

Figure 82 indicates that fully 50 percent of wireless operators did not experience any DDoS attacks on their networks during the last 12 months. The responses to this question were different than expected and provided our first clue that the visibility into the mobile networks is not actually as pervasive as the results originally led us to believe. The distribution of answers across this question was very unusual, as a significant number of respondents answered as having none or very few attacks per month, while another significant quantity answered as having over 50 attacks per month. This dichotomy of "a lot" versus "a little," with nothing in between, more likely represents the fact that the respondents do not have an accurate way of detecting and counting the number of attacks that they actually experience. We interpret this to be an artifact of the visibility caveats mentioned above.

DDoS Attacks per Month on Wireless Networks

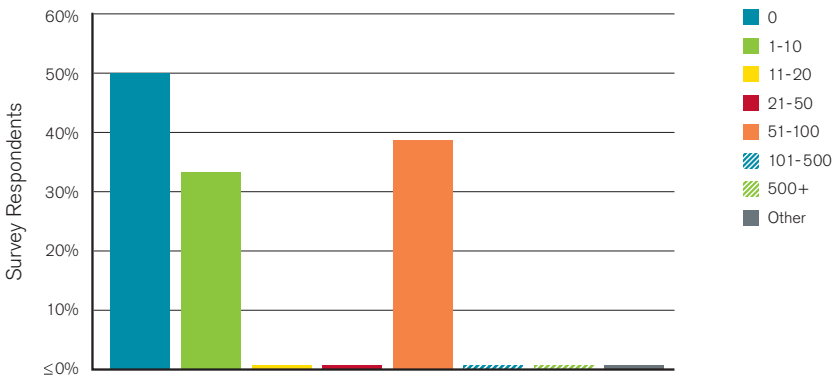

Figure 82 *Source: Arbor Networks, Inc.*

Sixty-three percent of respondents stated that they have experienced customer-visible outages during the survey period due to security incidents on their wireless networks (Figure 83).

Security Incidents Leading to Customer Outages

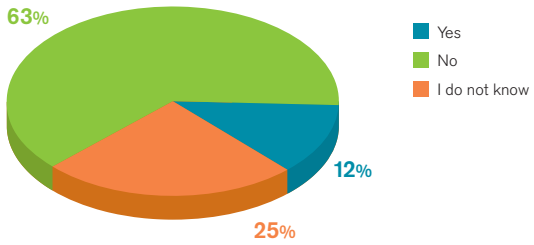

Figure 83 *Source: Arbor Networks, Inc.*

As illustrated in Figure 84, 80 percent of respondents indicated that their ancillary support infrastructure such as Web portals, DNS and other related services have been adversely affected by DDoS attacks over the 12-month survey period. Forty percent indicated that mobile handsets or end-customer computers with wireless connectivity have been affected by DDoS attacks.

Wireless Network Infrastructure Affected by DDoS Attacks

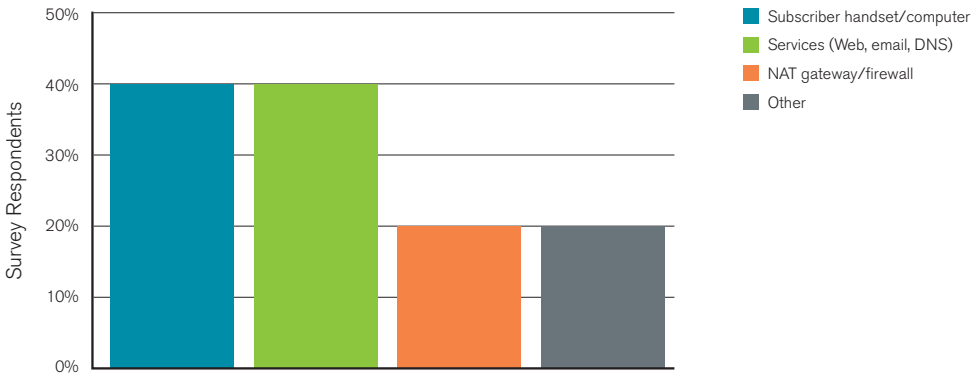

Figure 84 *Source: Arbor Networks, Inc.*

Nearly 24 percent of respondents indicated that stateful firewalls and/or stateful NAT devices on their networks have been adversely affected by DDoS attacks during the survey period (Figure 85). As mentioned in the "Data Center Operator Observations" section of this report (page 44), one can conclude that stateful firewall and/or IPS failure can be a deliberate or inadvertent result of DDoS attacks.

Observed DDoS Attacks Against Stateful Firewalls and/or NAT Devices in Wireless Networks

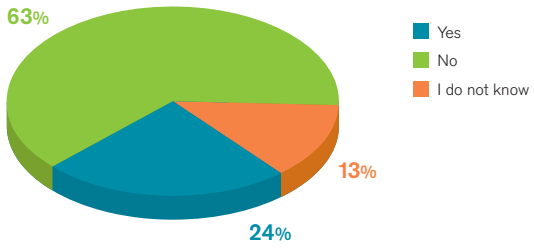

Figure 85 *Source: Arbor Networks, Inc.*

Figure 86 indicates that during the survey period, strong pluralities of respondents have experienced application-layer DDoS attacks directed at their supporting ancillary infrastructure elements. These elements include DNS servers, Web portal servers, SMTP servers, VoIP infrastructure, mobile IP infrastructure and SMS gateways. It is likely that at least some portion of the 50 percent of respondents who reported no application-layer DDoS attacks on their wireless networks during the 12-month survey period were unable to detect and classify such attacks due to limitations on network visibility.

Application-Layer DDoS Attacks Against Wireless Network Infrastructure

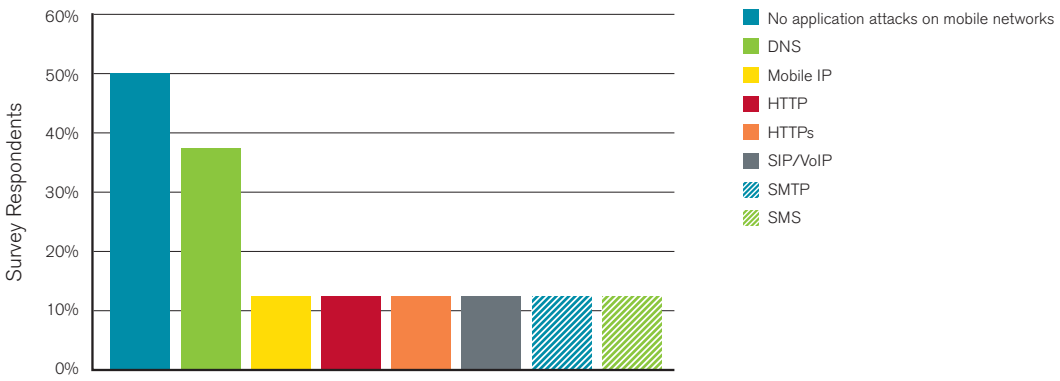

Figure 86 *Source: Arbor Networks, Inc.*

As illustrated in Figure 87, approximately 36 percent of respondents indicated that they have observed outbound/crossbound DDoS attacks originating from botted or abused subscriber nodes. This statistic may also be understated due to the network visibility limitations.

Outbound/Crossbound Attacks from Wireless Subscribers

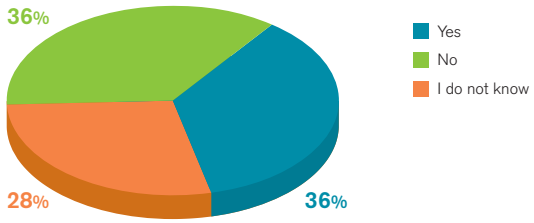

Figure 87 *Source: Arbor Networks, Inc.*

Figure 88 illustrates that well over 40 percent of respondents are unaware of what percentage of their subscriber base may be compromised and participating in botnets. A small percentage of respondents believe that more than 5 percent of their subscriber base is compromised. This finding supports the conclusion that while there have been significant strides towards improving visibility in mobile networks, the ability to do fine grained analysis and detection down to the host level is still not where it should be.

Percentage of Wireless Subscriber Nodes Participating in Botnets

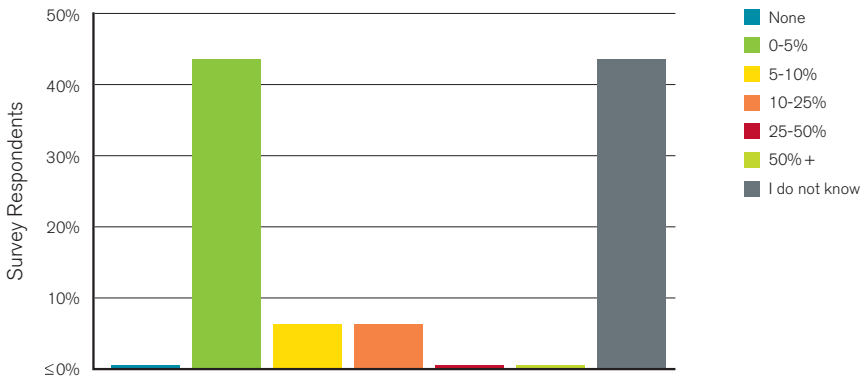

Figure 88 *Source: Arbor Networks, Inc.*

While Figure 89 purports to illustrate that at least 50 percent of respondents have not experienced DDoS attacks at Gi demarcation points in their network, it is important to note that nearly 38 percent of respondents indicated that they do not have sufficient visibility into their network traffic to detect and classify DDoS attacks at the Gi demarcation point. This again supports the point that visibility in mobile networks has still not reached a point of maturity.

DDoS Attacks Targeting Gi Demarcation

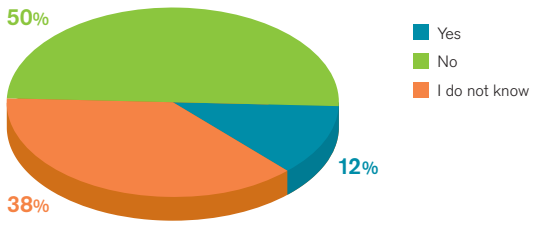

Figure 89 *Source: Arbor Networks, Inc.*

In this event, it turned out that we had inadvertently made a hidden assumption in the survey questions. That is, in framing some of the questions in this portion of the report, we had assumed that respondents had good visibility into network traffic on the wireline portions of their networks. In actuality, due to limitations in visibility on both the wireline and wireless portions of their networks, respondents were providing consistent responses. They were saying that a) they had roughly equivalent visibility between the wireline and wireless portions of their networks and that b) a significant minority of operators continue to face serious network visibility challenges in both the wireless and wireline portions of their networks. We also conclude that while having visibility equal to that of the wireline network is important, there are aspects to the mobile network that are quite unique, including data encapsulation and mobile-specific command and control protocols. While seeing this data is important, tools are needed to look deeper into the data and detect threats that operate within individual streams of traffic.

Having resolved this apparent contradiction in survey responses, in future editions of the report we will rephrase the relevant questions to remove any possibility for ambiguity.

Wireless operators listed stateful firewalls as a primary security measure to safeguard their packet cores, despite their limitations as a security technology, as previously discussed (Figure 90). Approximately 74 percent of respondents indicated they have deployed stateful firewalls in their networks as a defensive measure, a 17 percent increase year over year. Some 42 percent of respondents have made use of organic security capabilities built into their data and signaling gateways, and nearly 37 percent have deployed IDMS, a 13 percent increase over last year.

Security Measures Deployed on Wireless Networks

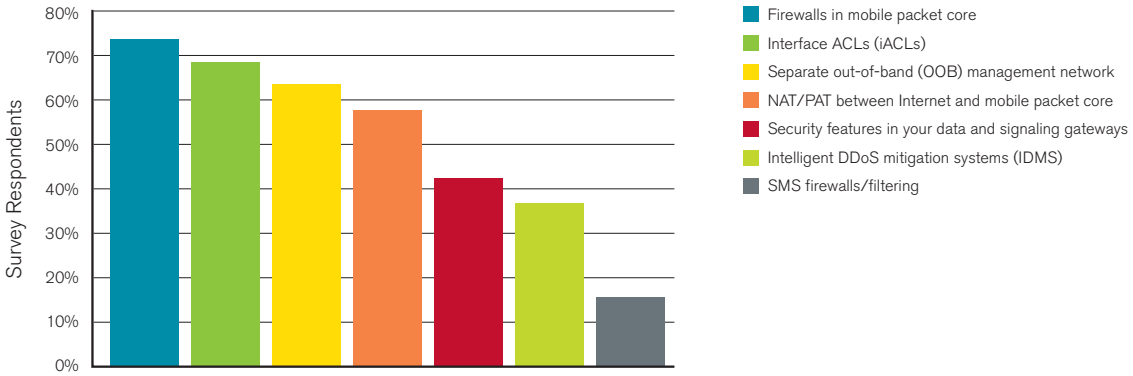

Figure 90 *Source: Arbor Networks, Inc.*

Figure 91 illustrates that 50 percent of respondents indicated that they intend to deploy IPv6 addressing for wireless subscriber nodes within the next 12 months, while nearly 41 percent have no plans to do so at this time. Approximately 9 percent of respondents have already deployed IPv6 on their production mobile networks.

In many cases, the security postures of mobile and fixed wireless operators continue to approximate those of wireline operators a decade or more ago. As discussed in the section of this report entitled "Data Center Operator Observations" (page 44), the failure of firewall and IPS devices to protect mobile and fixed wireless operators from DDoS attacks suggests that these devices are not well-suited for this application and that other solutions such as IDMS should be considered.

IPv6 Addressing Deployed for Wireless Subscribers/Infrastructure

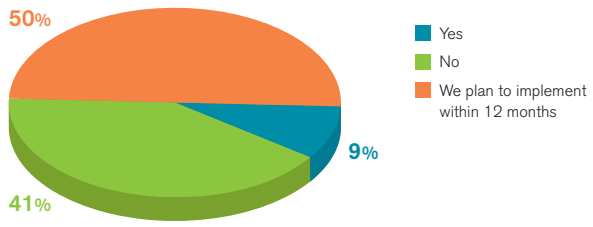

Figure 91 *Source: Arbor Networks, Inc.*

DNS and DNSSEC Migration Observations

More than 87 percent of respondents operate DNS servers on their networks (Figure 92). Over 77 percent have either assigned responsibility for their DNS infrastructure to their main operational security group or to a dedicated DNS security team (Figure 93).

DNS Server in Operation

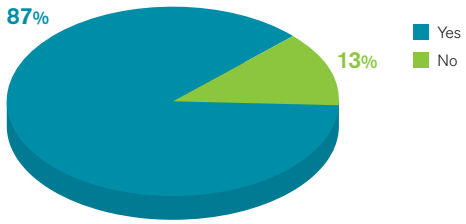

Figure 92 *Source: Arbor Networks, Inc.*

DNS Security Responsibility

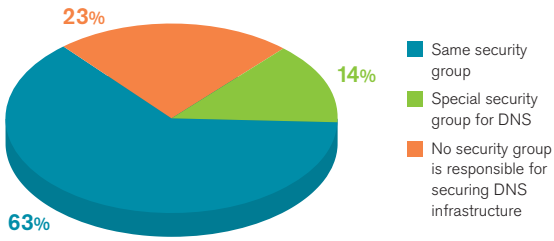

Figure 93 *Source: Arbor Networks, Inc.*

Nearly 23 percent of respondents indicate that there is no security group within their organizations with formal responsibility for DNS security. This may be a contributing factor to the significant number of unsecured, open DNS resolvers on the Internet today that can be abused by attackers to launch extremely high-bandwidth DNS reflection/amplification attacks. Such attacks continue to constitute the majority of 10 Gbps and greater DDoS attacks.

Approximately 78 percent of respondents have implemented the BCP of restricting recursive lookups by their DNS servers to queries located either on their own networks or on those of their end customers, while some 22 percent have not yet done so (Figure 94).

DNS Recursive Lookups Restricted

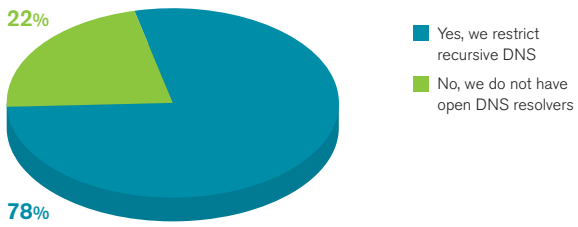

Figure 94 *Source: Arbor Networks, Inc.*

As indicated in Figure 95, approximately 12 percent of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period, a significant decrease over the last year. This may be a result of more operators beginning to take the necessary architectural, operational, scalability and attack mitigation measures to maintain availability in the face of attack. DNS has been both an attack target and vector of choice for attackers. Attacking the authoritative DNS servers for a given server or domain is often the easiest way to take it offline. Such an attack renders the relevant records of the DNS resource unresolvable to Internet users. In many cases, it also requires far fewer attack resources to disrupt service than would attacking the target servers/applications directly. The reduction in the percentage of customer impacting DDoS attacks is a good sign that DNS operators are beginning to take DDoS into consideration as they build out their DNS infrastructure.

Unfortunately, the DNS servers themselves are still being used as a means to attack others. The large number of misconfigured DNS open recursors on the Internet, coupled with the lack of anti-spoofing deployments, allows attackers to launch overwhelming multi-Gbps DNS reflection/amplification attacks.

Customer-Visible DNS Outages Due to DDoS Attacks

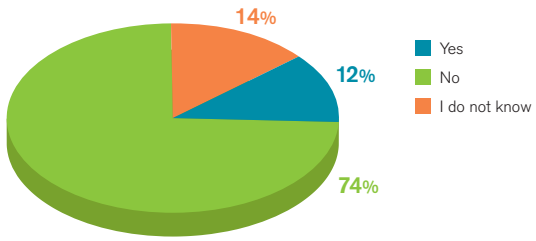

Figure 95 *Source: Arbor Networks, Inc.*

DNS Cache-Poisoning Attacks Observed

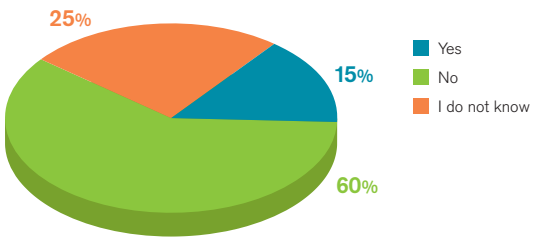

Figure 96 *Source: Arbor Networks, Inc.*

Only about 15 percent of respondents reported experiencing DNS cache-poisoning attacks directed to or through their DNS infrastructures during the survey period (Figure 96). Surprisingly, however, some 25 percent indicated that they do not know whether or not they have experienced these attacks, which reveals a serious gap in DNS server operator visibility.

As noted in Figures 97 and 98 respectively, 20 percent of respondents indicated that they had experienced DDoS attacks against recursive DNS servers during the last 12 months, while nearly 24 percent indicated they had experienced attacks against authoritative DNS servers during the survey period. Over 18 percent noted that they did not know whether they had experienced such attacks during the survey period; this further reinforced the notion that DNS server operators should prioritize improvements to their DNS traffic visibility.

DDoS Attacks Against Recursive DNS Servers

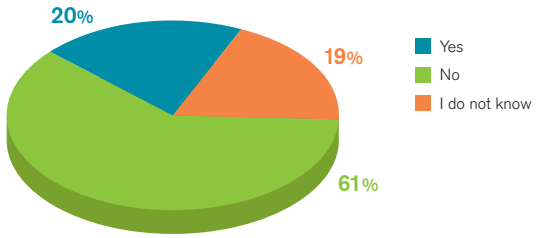

Figure 97 *Source: Arbor Networks, Inc.*

DDoS Attacks Against Authoritative DNS Servers

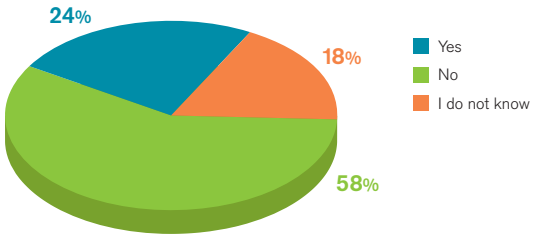

Figure 98 *Source: Arbor Networks, Inc.*

In a significant positive change over the last 12 months, 37 percent of respondents reported plans to implement DNSSEC within the next 12 months, while over 22 percent have already begun deployment and nearly 9 percent indicated full deployment on their networks (Figure 99).

DNSSEC Deployment Status

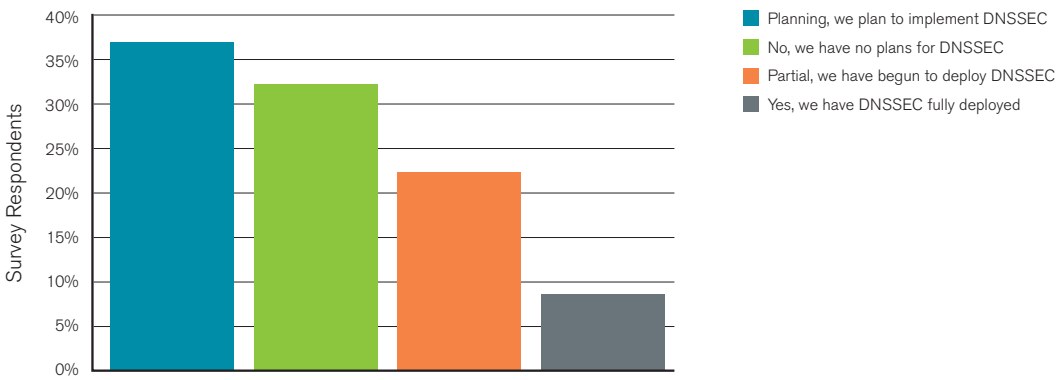

Figure 99 *Source: Arbor Networks, Inc.*

As illustrated in Figure 100, approximately 46 percent 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. However, an alarming 45 percent indicated that they have insufficient visibility to make this determination, which reveals another very serious gap in DNS operator traffic analysis capabilities.

DNSSEC Infrastructure Support Issues

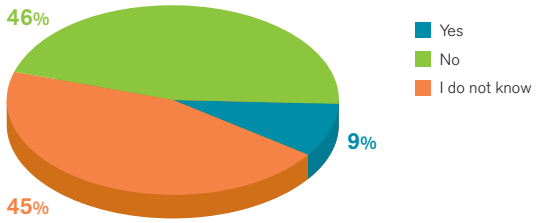

Figure 100 *Source: Arbor Networks, Inc.*

Concerns Regarding DNSSEC Response Sizes Enabling DNS Reflection/Amplification DDoS Attacks

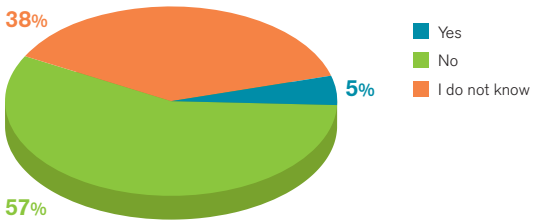

Figure 101 *Source: Arbor Networks, Inc.*

Fifty-seven percent of respondents indicated they do not believe that drastically increased DNS response sizes would present a new and even more easily abused vector for DNS reflection/amplification attacks (Figure 101). As noted in last year's report, DNSSEC-enabled DDoS attack amplification has been observed in the wild, in contrast with respondent views. When asked if they had additional concerns regarding DNSSEC deployment, respondents provided the following feedback:

- "Deployment is too slow—we need greater adoption! We're actively working to encourage and assist our customers in deploying DNSSEC."
- "Folks don't generally understand the baggage that comes along with DNSSEC—it's a learning process."
- "DNSSEC is very complicated. Will be a mess to operate/support."
- "Complex to implement, hard to get it working right. People currently implementing seem not to take it too seriously, and outages have been known at TLD level due to expired keys, misconfigurations, etc."
- "Not enough people are using DNSSEC. The last-mile hop suffers from a gap in security to stub resolvers and forwarders."

VoIP Observations

Approximately 47 percent of respondents indicated that they offer VoIP services to their end customers (Figure 102). Of that respondent pool, nearly 30 percent indicated that there is no security group within their organizations with formal responsibility for securing the VoIP service delivery infrastructure (Figure 103), a 10 percent reduction year over year.

Offered VoIP Services

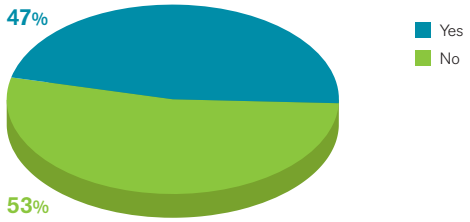

Figure 102 *Source: Arbor Networks, Inc.*

VoIP Security Responsibility

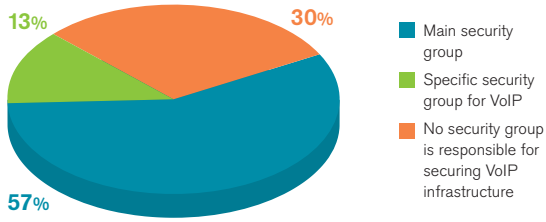

Figure 103 *Source: Arbor Networks, Inc.*

As noted in Figure 104, over 46 percent of respondents operating VoIP services observed toll fraud taking place in their VoIP infrastructures during the survey period. Of those who observed VoIP toll fraud, approximately 42 percent noted that attackers utilized brute-force attack techniques to commit toll fraud (Figure 105). Attackers often use these techniques in such volume that they constitute an inadvertent DDoS attack on the VoIP infrastructure and result in service outages.

Toll Fraud Observed on VoIP Services/Infrastructure

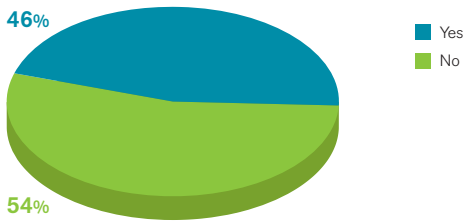

Figure 104 *Source: Arbor Networks, Inc.*

Brute-Force Attack Techniques Observed in VoIP Toll Fraud

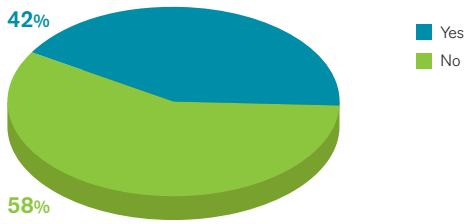

Figure 105 *Source: Arbor Networks, Inc.*

Nearly 63 percent of respondents indicated that caller ID spoofing is a serious concern with regards to their VoIP infrastructure (Figure 106).

Concerns Regarding Caller ID Spoofing on VoIP Services

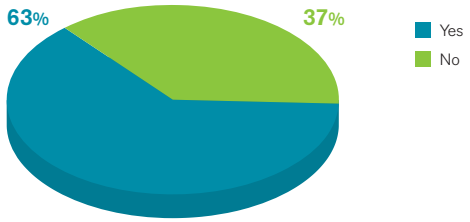

Figure 106 *Source: Arbor Networks, Inc.*

As illustrated in Figure 107, approximately 37 percent of respondents stated that they use commercial tools to detect attacks against their VoIP infrastructure; nearly 32 percent make use of open-source tools; and over 29 percent utilize homegrown detection tools. Meanwhile, almost 27 percent of respondents indicated that they do not have access to any attack detection tools for use on their VoIP infrastructure.

Tools Used to Detect VoIP Attacks

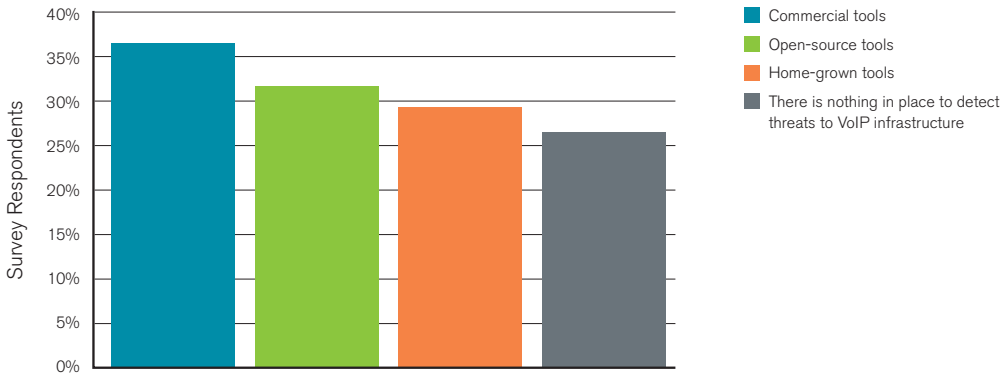

Figure 107 *Source: Arbor Networks, Inc.*

Figure 108 illustrates that some 36 percent of this pool of respondents indicated that they use firewalls as their primary defense mechanism against DDoS attacks. More than 15 percent rely on iACLs, while over 23 percent utilize IDMS, a 7 percent increase over last year.

Primary Tool Used to Mitigate DDoS Attacks Against VoIP Services/Infrastructure

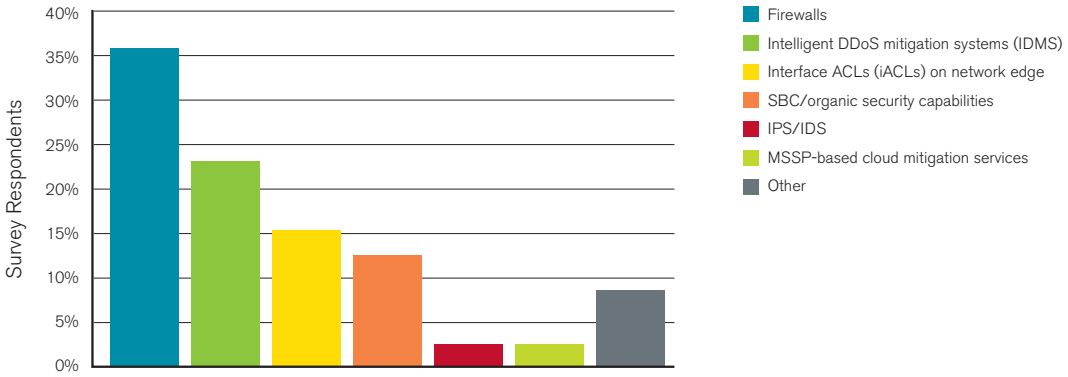

Figure 108 *Source: Arbor Networks, Inc.*

Over 63 percent of respondents indicated that they utilize SBCs in their VoIP infrastructure (Figure 109). Nearly 59 percent stated that they use additional tools (such as S/RTBH) and IDMS to protect their SBCs against DDoS attack (Figure 110).

SBCs Deployed

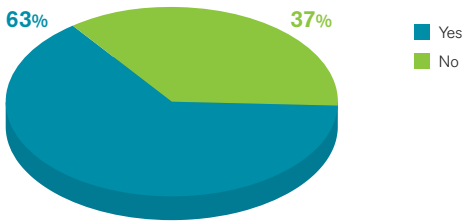

Figure 109 *Source: Arbor Networks, Inc.*

SBCs Protected Against DDoS by Additional Tools/Techniques

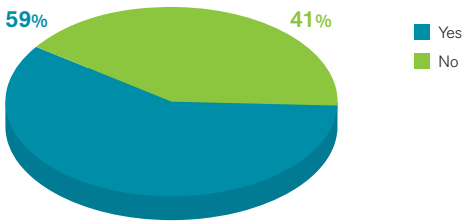

Figure 110 *Source: Arbor Networks, Inc.*

Respondent Survey Feedback

We asked survey respondents to provide us with their views regarding this year's survey, as we do every year.

The feedback we received was generally positive and constructive, as noted below:

- "Thank you very much for the invitation to participate."
- "Would be nice if the survey asked more specifics about DDoS attack details so that Arbor can compile and release even more detailed information in the yearly report (i.e., average attack size in bps and pps, attack type [SYN flood, DNS, ICMP])."
- "Oh, it's kind of embarrassing how far behind the curve we are!"
- "Was long. :)"
- "I think you can explore IPS with more detail."
- "There are too many questions versus responsibility for a company as large as ours."
- "Nice survey. Thanks!"

As always the responses and information received from survey participants is very appreciated. This open survey feedback helps us to continually improve the quality of this report.

Conclusions

This seventh edition of the Arbor Networks® *Worldwide Infrastructure Security Report* contains several significant data points that highlight important trends in attacker methodologies and network operator challenges.

In this year's report, we note that flood-based DDoS attacks in the 10 Gbps range have become increasingly prevalent, indicating that network operators must be prepared to routinely mitigate such high-volume attacks. Respondent data also reveals that attackers are more readily making use of sophisticated multi-vector DDoS attacks and complex application-layer attack methodologies to further their goals.

Respondent organizations provided the first documented evidence of IPv6 DDoS attacks on production networks. The relative rarity of IPv6 DDoS attacks signifies that the operational and economic significance of IPv6 remains low, despite increased deployment efforts. Awareness of the threat posed by DDoS attacks has risen significantly during the survey period, with experience as the target of a DDoS attack being the most common factor behind this heightened awareness. Data center operators continue to suffer outages related to the failure of stateful firewalls, IPS devices and load-balancer devices due to DDoS attacks. Mobile and fixed wireless operators should re-assess their network visibility capabilities in light of the self-contradictory data in this year's report.

Finally, in what may be the most significant finding in this year's report, ideology and "hacktivism" have emerged as the number-one motivating factor behind DDoS attacks, followed by disputes related to online gaming. Network operators and end-customers alike must ensure that their risk assessment models and situational awareness capabilities reflect this new reality.

About the Authors

Roland Dobbins, Solutions Architect for Asia Pacific, Arbor Networks
rdobbins@arbornetworks.com

Roland Dobbins has 26 years of operational experience in the service provider and large enterprise arenas. His experience includes designing, deploying, operating, securing, maintaining, troubleshooting and defending many of the highest-visibility networks in the world.

Mr. Dobbins is a recognized industry leader in the fields of operational security and network telemetry. He has an extensive background in security product/feature innovation, devising operational security requirements for network infrastructure devices and protocol design. His focus is on extending the availability, scalability and security of the network infrastructure and the applications/services it enables, with an emphasis on flexible and resilient global service delivery capabilities.

Carlos Morales, Vice President, Global Sales Engineering and Consulting, Arbor Networks
cmorales@arbornetworks.com

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. Mr. 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.

Mr. 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.

CONTRIBUTORS

Darren Anstee, Solutions Architect for EMEA, Arbor Networks
danstee@arbornetworks.com

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.

Julio Arruda, Senior Manager, Latin American Consulting Engineering, Arbor Networks
jarruda@arbornetworks.com

Julio Arruda has more than 20 years of experience in the networking and telecommunications industry. In his current role at Arbor, he manages the consulting engineering team for the Latin American region. Arruda brings an in-depth familiarity with the Caribbean and Latin American Internet and telecom environments, along with broad knowledge of diverse telecommunication technologies. Prior to joining Arbor, he worked in the professional services organization at Bay Networks, and later as network engineer at Nortel Networks.

Tom Bienkowski, Director of Product Marketing, Arbor Networks
tbienkowski@arbornetworks.com

Tom Bienkowski has more than 20 years of experience in the networking and security industry. At Arbor, he directs product marketing for the fixed and mobile service provider markets. Prior to joining Arbor, Bienkowski worked for large enterprises as a network engineer and for multiple network management and security vendors, where he had roles in sales engineering, technical field marketing and product management.

Michael Hollyman, Manager of Consulting Engineering, Arbor Networks
mhollyman@arbornetworks.com

With more than 12 years in the network, security and telecommunications industries, Mike Hollyman brings extensive knowledge of service provider and large enterprise network design and security to Arbor. He provides leadership to the Arbor sales organization through his management of the company's consulting engineering team for North American service providers. Prior to joining Arbor, Hollyman was a network and security consultant, both independently and through his own consulting company. He also worked as a network engineer for OneSecure, Qwest Communications and the University of Illinois.

Dr. Jose Nazario, Senior Manager of Security Research, Arbor Networks
jnazario@arbornetworks.com

Jose Nazario is senior manager of security research at Arbor Networks. In this capacity, he is responsible for analyzing burgeoning Internet security threats, reverse engineering malicious code, managing software development and developing security mechanisms that are distributed to Arbor Peakflow platforms via Arbor's Active Threat Feed (ATF) threat detection service. Dr. Nazario's research interests include large-scale Internet trends such as reachability and topology measurement; Internet-scale events such as DDoS attacks, botnets and worms; source code analysis tools; and data mining. He is the author of the books "Defense and Detection Strategies against Internet Worms" and "Secure Architectures with OpenBSD." He earned a Ph.D. in biochemistry from Case Western Reserve University in 2002. Prior to joining Arbor Networks, he was an independent security consultant. Dr. Nazario regularly speaks at conferences worldwide, with past presentations at CanSecWest, PacSec, Black Hat and NANOG. He also maintains WormBlog.com, a site devoted to studying worm detection and defense research.

Edwin Seo, Regional Manager, Asia Pacific Sales Engineering, Arbor Networks
eseo@arbornetworks.com

Edwin Seo brings more than 12 years of experience in service provider networking, infrastructure and security. Based in Singapore, he currently runs Arbor's systems engineering team for the Asia Pacific region. Prior to joining Arbor, Seo held various systems engineering leadership roles at Ellacoya Networks, Cisco Systems and StarHub.

Rakesh Shah, Director of Product Marketing and Strategy, Arbor Networks
rshah@arbornetworks.com

Rakesh Shah has been with Arbor since 2001, helping to take the company's products from early-stage to category-leading solutions. Before moving into the product marketing team, Shah directed product management for Arbor's Peakflow products and managed the engineering group. Previously, he held various engineering and technical roles at Lucent Technologies, PricewaterhouseCoopers and CGI/AMS.

Glossary

A

ACL	access control list
APAC	Asia Pacific
APNIC	Asia Pacific Network Information Centre
ATLAS	Active Threat Level Analysis System
AUP	acceptable use policy

B

BCP	best current practice
BGP	Border Gateway Protocol
BPDU	bridge protocol data unit

C

C&C	command-and-control
CAPEX	capital expenditure
CDN	content delivery network
CERT	computer emergency response team
CGN	carrier-grade NAT
CIDR	Classless Inter-Domain Routing
CPE	customer-premises equipment
CSIRT	computer security incident response team

D

DCN	dynamic circuit network
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DLP	data loss prevention
DNS	domain name system
DNSSEC	domain name system security extensions
DPI	deep packet inspection
D/RTBH	destination-based remotely triggered blackholing
DSL	digital subscriber line

E

eBGP	exterior Border Gateway Protocol
EDNS	extension mechanisms for DNS
EPP	Extensible Provisioning Protocol

F

FIRST	Forum of Incidence Response and Security Teams
FTP	File Transfer Protocol

G

Gbps	gigabits per second
GGSN	Gateway GPRS Support Node
Gi	GGSN-to-PDN
GPRS	General Packet Radio Service Tunneling Protocol
GTSM	generalized TTL security mechanism

H

HA	home agent
HTTP	Hypertext Transfer Protocol
HTTP/S	HTTP Secure

I

iACL	infrastructure ACL
IDC	Internet data center
IDMS	intelligent DDoS mitigation system
IDS	intrusion detection system
IGP	Internet Gateway Protocol
IPS	intrusion prevention system
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
IRR	Internet Routing Registry

L

LAN	local area network
LTE	Long Term Evolution

M

MVNO	mobile virtual network operator
MSO	multiple service operators

N

NAT	network address translator
NMS	network management system
NOC	network operations center

O

OOB	out of band
OPEX	operational expenditure
OPSEC	operational security
OSS	operations support system

Glossary (continued)

P

PACL	port ACL
PAT	port address translation
PDN	public data network
PHP	Hypertext Preprocessor
POP	Post Office Protocol
pVLAN	private virtual LAN

Q

QoS	quality of service

R

RAN	radio access network
RDP	Remote Desktop Protocol
RIR	regional Internet registry
ROI	return on investment

S

SBC	session border controller
SGSN	Serving GPRS Support Node
SHA-1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol
SLA	service level agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	security operations center
SQL	Structured Query Language
S/RTBH	source-based remotely triggered blackholing
SSH	secure shell
SSL	Secure Sockets Layer

T

TCP	Transmission Control Protocol
TTL	time to live

U

UTM	unified threat management
uRPF	Unicast Reverse Path Forwarding

V

VACL	VLAN ACL
VLAN	virtual LAN
VOD	voice on demand
VoIP	Voice over Internet Protocol
VPN	virtual private network

W

WiMAX	Worldwide Interoperability for Microwave Access

Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824

Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 208 622 3108

Asia Pacific

T +65 6299 0695

www.arbornetworks.com

ARBOR® NETWORKS

SR/WISR/EN/0212