VOLUME VI

Worldwide Infrastructure Security Report

2010 Report

ARBOR® NETWORKS

Table of Contents

List of Figures

Overview

Arbor Networks®, in cooperation with the Internet operational security community, has completed the sixth edition of an ongoing series of annual operational security surveys. This survey, covering roughly a 12-month period from October 2009 through September 2010, 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 trends and employment of various infrastructure security techniques. 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 than theoretical and emerging attack vectors addressed and speculated about elsewhere.

Key Findings

Network Operators Face Larger, More Frequent Attacks as Attackers Redouble Their Efforts

After a respite in the growth of packet-flooding DDoS attack bandwidth during the 2008 to 2009 survey period, attackers have moved aggressively over the current survey period to dramatically increase attack volumes—for the first time launching DDoS attacks breaking the 100 Gbps barrier. This represents a 102 percent increase in DDoS attack bandwidth since the previous survey period and a staggering 1000 percent increase since Arbor released the first *Worldwide Infrastructure Security Report (WISR)* in 2005. Figure 1 illustrates the yearly reported maximum attack size.

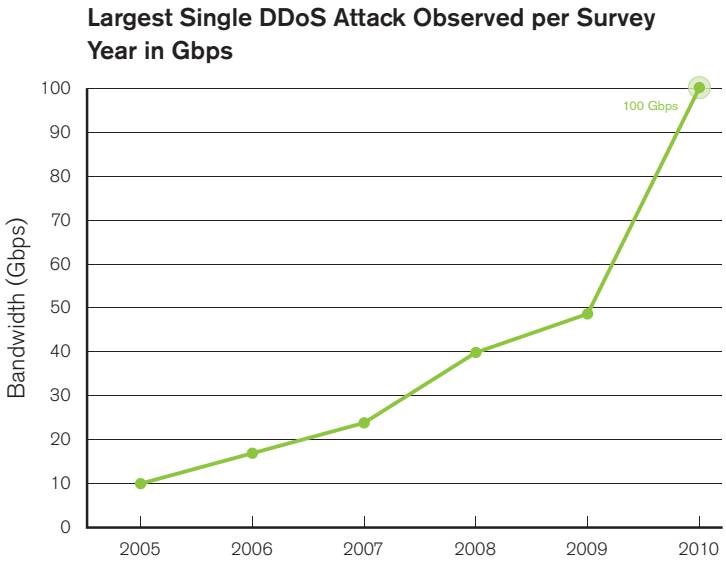

Figure 1
Source: Arbor Networks, Inc.

Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact

IDC and mobile/fixed wireless operators in particular are reporting significant outages, increased OPEX, customer churn and revenue loss due to application-layer DDoS attacks. These attacks are targeting both their customers and their own ancillary supporting services, such as DNS, Web portals, etc.

Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks

Mobile and fixed wireless operators are reporting that they have little visibility into traffic on their networks and even less ability to influence that traffic. With some notable exceptions, many mobile/fixed wireless network operators appear to have security postures approximating those of wireline operators some 8 to 10 years ago.

Firewalls and IPS Devices Are Falling Short on DDoS Protection

Mobile/fixed wireless operators, IDCs and VoIP operators appear to be making many of the same architectural and operational choices that wireline operators made early in the decade. Notably, they have deployed stateful firewalls and IPS devices in their networks. In light of the growth in application-layer DDoS attacks, such devices frequently lower the overall security postures of operators by acting as stateful DDoS chokepoints—rendering networks more susceptible to both deliberate and inadvertent DDoS attacks.

DDoS Attacks Have Gone Mainstream

The mainstream media has extensively reported numerous high-profile DDoS attacks motivated by political or ideological disputes. These include DDoS attacks associated with the WikiLeaks[1] affair, the territorial disputes between China and Japan, and the ongoing political turmoil in Burma[2] and Sri Lanka. In 2010, protecting availability has forcefully made it onto the radar screen of enterprise IT consulting firms worldwide, and DDoS defense has consequently reached the status of a CXO-level issue globally.

DNS Has Broadly Emerged as an Attack Target and Enabler

Due to the relatively limited attention given to DNS protection and scalability by many network operators, DNS attacks have emerged as one of the easiest ways to take servers, services or applications offline by denying Internet users the ability to resolve the relevant DNS resource records. Additionally, the large number of misconfigured DNS open recursors present on the Internet, coupled with insufficient edge anti-spoofing technology deployments on many networks, allows attackers to launch overwhelming DNS reflection/amplification attacks.

Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge

Operators who have deployed IPv6 are expressing numerous concerns regarding visibility into IPv6 traffic on their networks, as well as their ability to exert as much control over IPv6 traffic as they currently do over IPv4 traffic. The additional network state and DDoS vectors necessitated by the deployment of 6-to-4 gateways and carrier-grade NATs are also significant threats to availability.

Chronic Underfunding of Operational Security Teams

Nontechnical factors, driven by a lack of understanding and commitment, continue to represent the most significant obstacles to reducing mitigation times and proactively strengthening operational security postures. These factors include a shortage of skilled resources, communications siloing, and poorly defined operational responsibilities and policies.

Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement

Most operators do not report operational security incidents to law enforcement. This is due to both a lack of network operator resources and a lack of confidence in the ability of law enforcement to successfully investigate these incidents, especially in a multijurisdictional context.

Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Most operators welcome the involvement of governments in setting up national CERTs, and believe that government can and should play a more active role in operational security matters. However, operators overwhelmingly express low confidence in the efficacy of government efforts to date surrounding critical infrastructure protection.

1 http://asert.arbornetworks.com/2010/11/wikileaks-cablegate-attack
2 www.irrawaddy.org/highlight.php?art_id=20406

Demographics of Survey Respondents

Survey participants included 111 self-classified Tier 1, Tier 2 and other IP network operators (Figure 2) from the US and Canada, Latin/South America, EMEA, Africa and Asia. Figure 3 (below) and Figure 4 (page 8) illustrate that while the number of respondents decreased slightly from the 2009 report, geographical diversity and operational focus diversity (Figure 5, page 8) increased year over year.

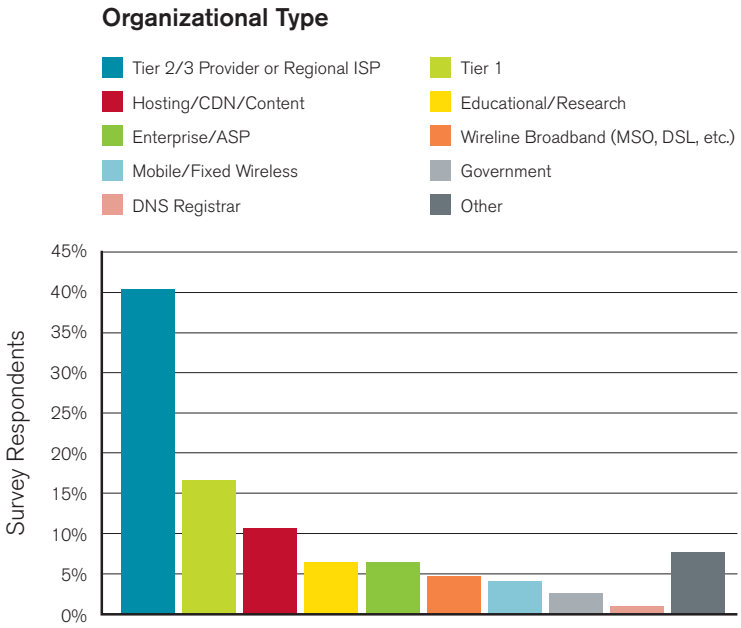

Figure 2
Source: Arbor Networks, Inc.

As illustrated in Figure 2, this year's respondent pool saw a major demographic shift toward Tier 2 and Tier 3 regional providers; hosting/CDN/content providers; and mobile/fixed wireless operators. One reason for this apparent shift is because operators who offer multiple lines of business, such as wireline transit and mobile/fixed wireless access, were asked to self-report as Tier 2. The "Other" category includes pure managed service providers, security researchers actively engaged in the global operational security community and financial application service providers.

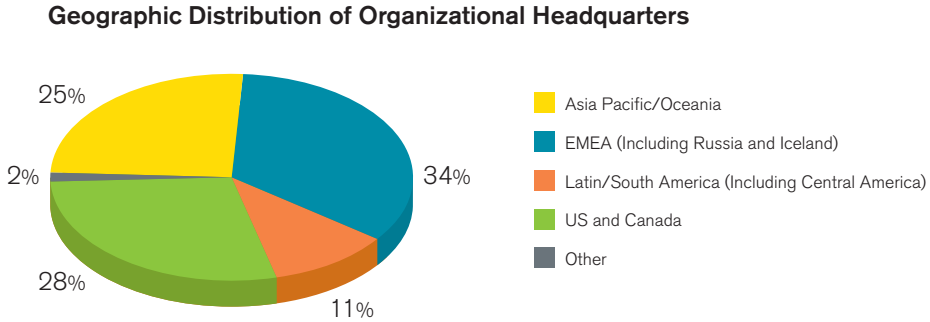

Figure 3
Source: Arbor Networks, Inc.

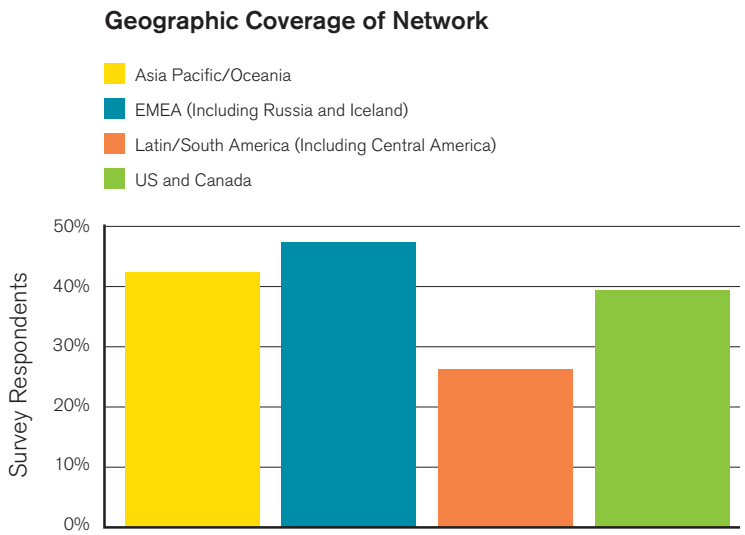

Figure 4
Source: Arbor Networks, Inc.

All survey participants are directly involved in network security operations at their respective organizations (Figure 5) and/or make direct contributions to the global operational security community. Once again, the increased diversity of geographical presence and operational focus has an impact on various results and observable trends over the six-year survey lifetime—something we attempt to highlight accordingly where considered pertinent.

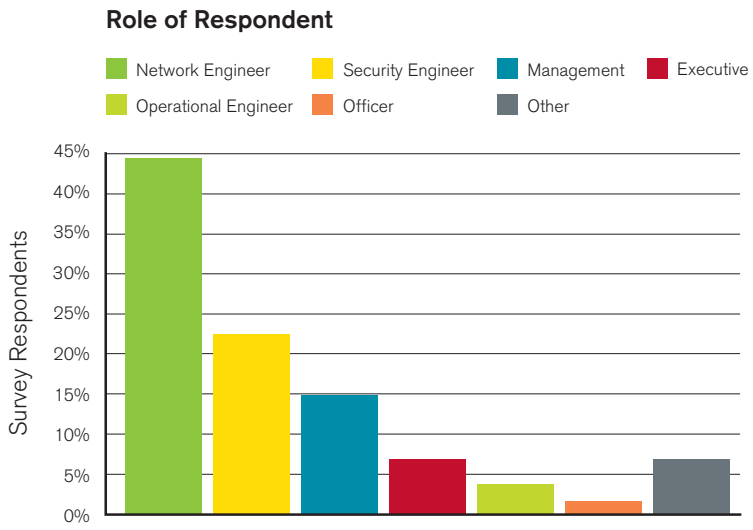

Figure 5
Source: Arbor Networks, Inc.

A strong plurality of respondents self-identified their specific job role as that of network engineer, while security engineers and management were represented in second and third places, respectively. In addition to the titles listed in Figure 5 (page 8), additional job categories included security architects, security analysts, security researchers, managed security services product managers and an e-crime manager, which to date is a unique title in the history of the *Worldwide Infrastructure Security Report*.

Figure 6 illustrates that 35 percent of respondents offer mobile/fixed wireless broadband access and 43 percent offer managed security services. In addition to the specific services described in Figure 6, some respondents also offer VOD services, e-government-focused services, IPv6 tunnel-broker services and EPP registry services.

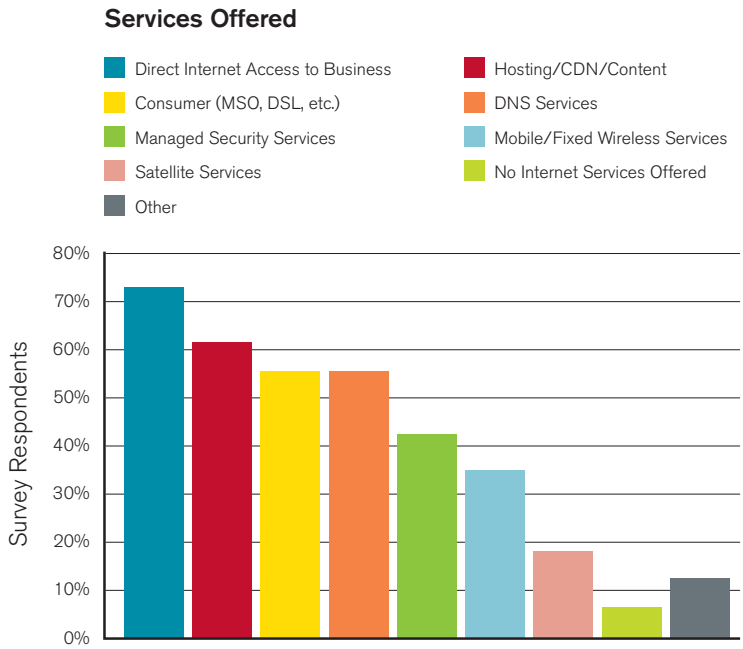

Figure 6
Source: Arbor Networks, Inc.

Survey Methodology

This edition of the survey consisted of 113 free-form and multiple-choice questions, representing an 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 IDC operators, as well as mobile and fixed wireless operators.

All data is presented in an aggregate and anonymous manner, and provided with the permission of the respondents. Individual respondents were typically senior network security architects or operations engineers at their respective organizations. 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.

Note: As in previous reports, several survey questions included multiple selections and you will note that the same applies to this report.

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 polled network security or 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; and 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

Sixty-eight percent of respondents indicated that DDoS attacks toward end customers were a significant operational threat encountered during this 12-month survey period (Figure 7). Interestingly, 61 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' ancillary support services, such as DNS, Web portals and email servers. Spam and VoIP-related attacks were also included in the "Other" category.

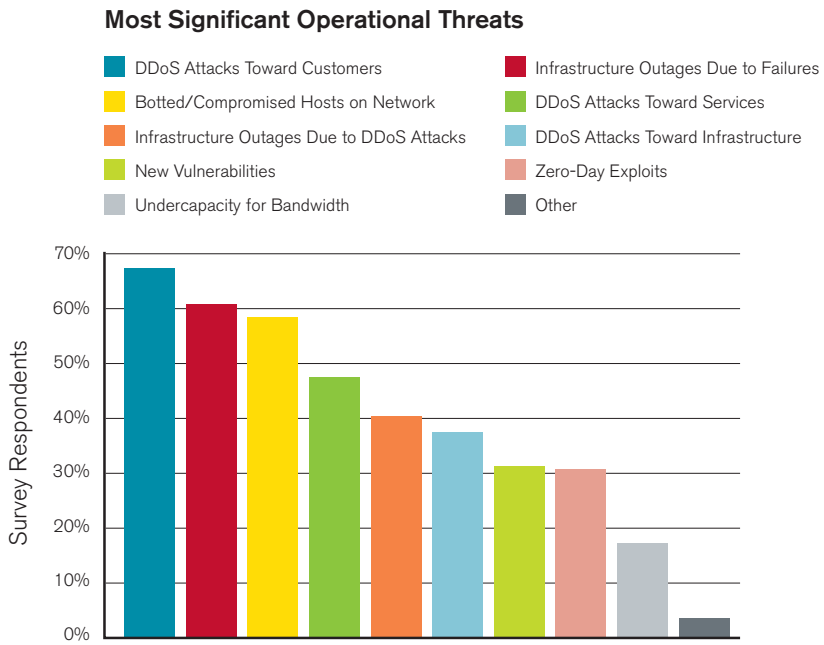

Figure 7
Source: Arbor Networks, Inc.

With regards to application-layer attacks (Figure 8, page 11), respondents listed HTTP, DNS and SMTP as the most-frequently targeted applications, with SIP/VoIP and HTTP/S coming in at fourth and fifth place, respectively. Our anecdotal experience working with operators over the last year indicates that: 1) attacks against the reputation of individual email senders, known as "joe jobs," are on the increase; and 2) both SMTP servers and commercial anti-spam systems have suffered serious losses of availability due to these incidents.

Targeted applications in the "Other" category include SSH, online gaming, FTP, Telnet, RDP, SQL databases, IRC, PHP and TCP port 123.

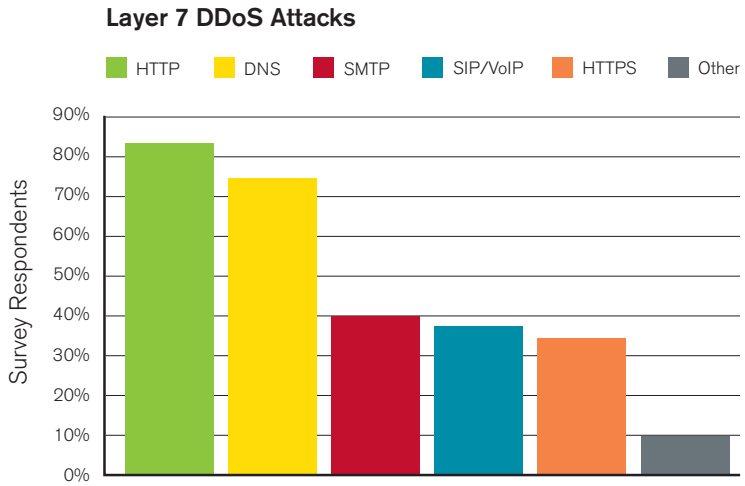

Figure 8
Source: Arbor Networks, Inc.

Top security concerns for the next twelve months (Figure 9) include attacks against end customers; attacks against operators' ancillary support services such as DNS and Web portals; attacks directed at operators' network infrastructure devices; botnet activities, which include DDoS attacks; and, interestingly, new vulnerabilities.

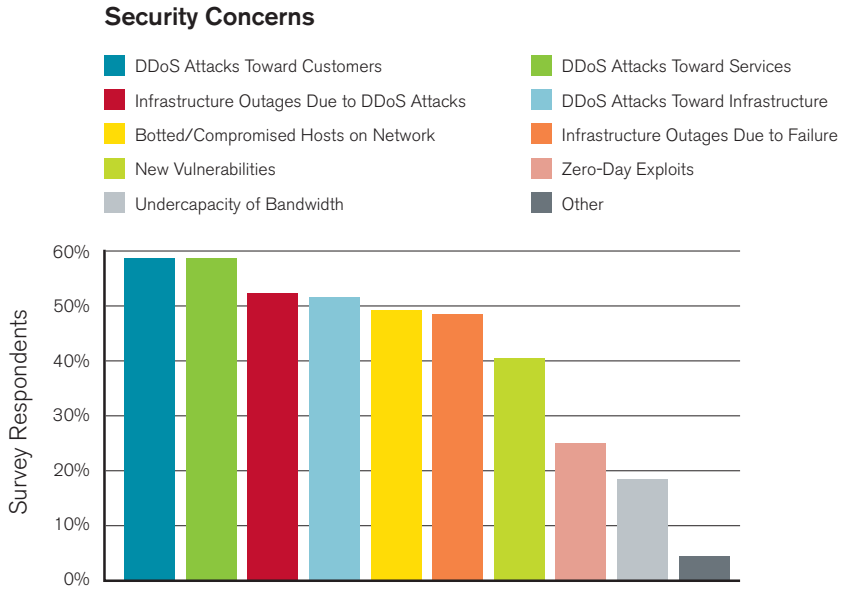

Figure 9
Source: Arbor Networks, Inc.

Based upon responses described later, we believe that the prominently highlighted concern over new vulnerabilities is in part related to the deployment of IPv6.

Other forward-looking security concerns expressed include VoIP-specific attacks and data loss/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.

Concerns Regarding Integrity of Infrastructure Vendor Products

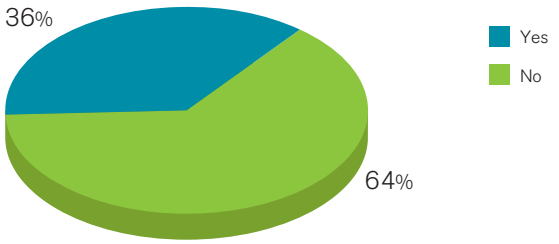

Figure 10
Source: Arbor Networks, Inc.

Influence of Integrity Concerns on Product Procurement

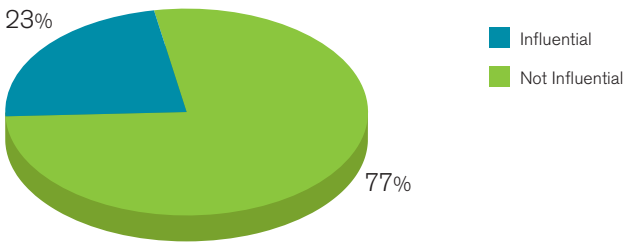

Figure 11
Source: Arbor Networks, Inc.

Respondents indicating concerns regarding product origins offered the following comments:

"We ensure we deal with established vendors in order to avoid this issue."

"Nation-state ownership of vendors is a concern."

"We've made some design choices with the intention of avoiding certain vendors."

By way of contrast, 76 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.

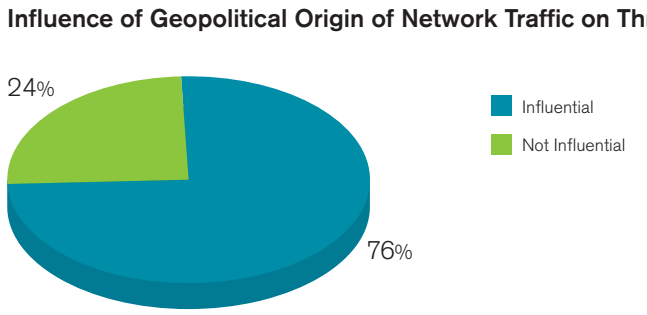

Figure 12
Source: Arbor Networks, Inc.

Scale, Targeting and Frequency of Attacks

As illustrated in Figure 1 (page 5) and again in Figure 13, the highest-bandwidth attack observed by respondents during the survey period was a 100 Gbps DNS reflection/amplification attack. This represents a 102 percent increase over the previous year. It is also the single largest increase in attack bandwidth year over year since the first report in 2005 and a 1000 percent increase in attack bandwidth since the report's inception.

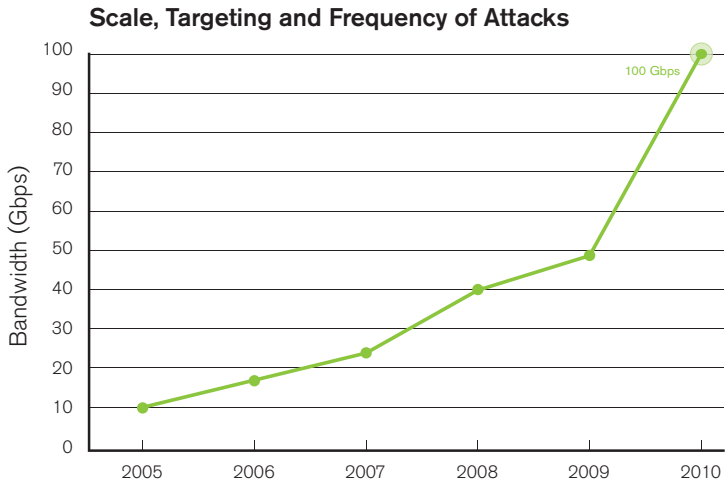

Figure 13
Source: Arbor Networks, Inc.

Based upon our experiences working with operators over the last year, we believe this large increase in attack-traffic bandwidth may be partially due to operators focusing their defenses against lower-bandwidth and application-layer DDoS attacks. Attackers may have had to "up the ante" to overwhelm the defenses and bandwidth capacity of defenders. Additionally, the increased availability of botted hosts, combined with the growing popularity of DNS amplification/reflection attacks, has also played a role in this escalation.

Sixty-five percent of respondents reported that the highest-bandwidth DDoS attack they experienced during this survey period was directed at their end customers, while 26 percent reported that their own ancillary support services such as DNS and Web portals were targeted (Figure 14). Eight percent indicated that their own network infrastructure was the target of the highest-bandwidth attack they experienced.

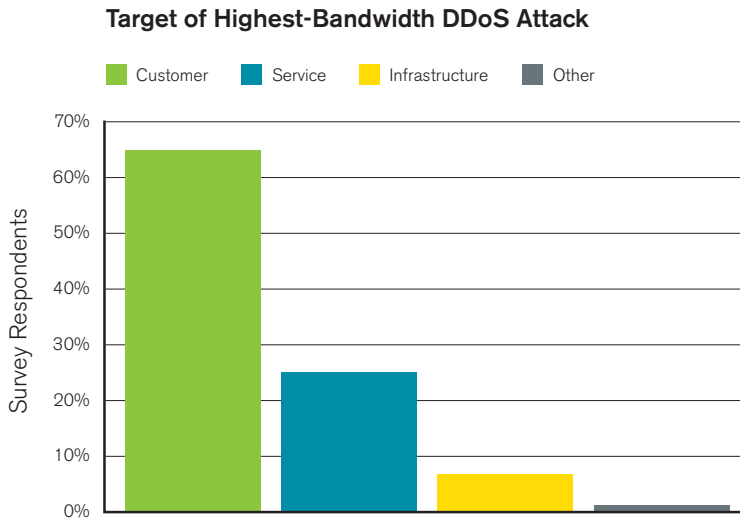

Figure 14
Source: Arbor Networks, Inc.

As shown in Figure 15, 47 percent of respondents indicated that they experienced 1 to 10 DDoS attacks per month during the survey period, while an additional 47 percent experienced 10 to 500 or more DDoS attacks per month.

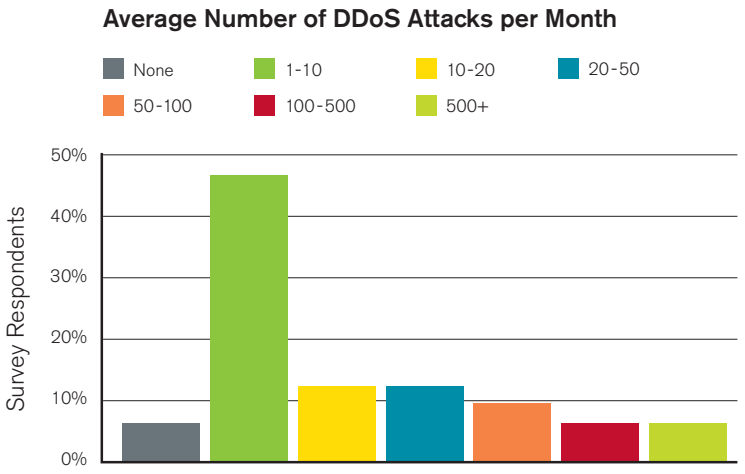

Figure 15
Source: Arbor Networks, Inc.

As illustrated in Figure 16, commercial flow-telemetry collection/analysis systems, such as the Arbor 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. Open-source flow-telemetry collection/analysis tools and custom in-house developed tools were the second- and third-most popular solutions in this category, respectively.

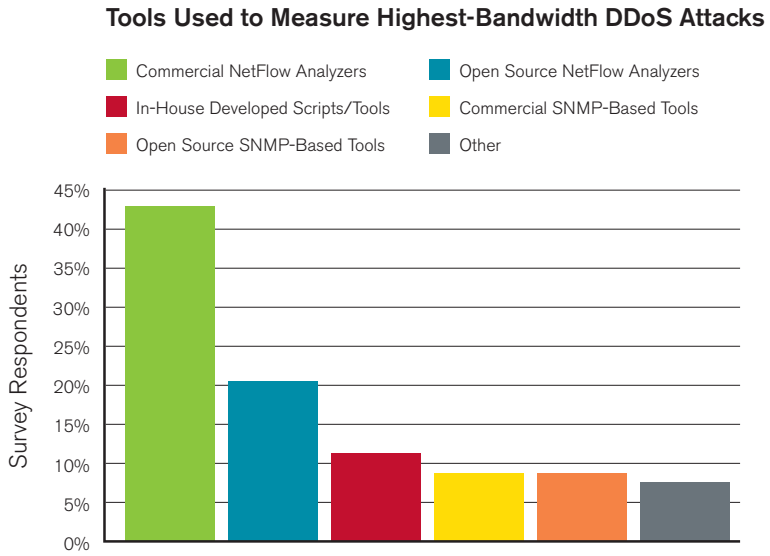

Figure 16
Source: Arbor Networks, Inc.

We have observed that it is a common misperception that DDoS attacks tend to originate outside one's own network. The reality is that compromised, botted hosts launching DDoS attacks can be located on one's own network—and that these outbound/crossbound DDoS attacks can be just as devastating to end customers and operators as inbound attacks originating from peers, upstream transit providers or downstream customers.

Figure 17 indicates that 73 percent of respondents detected and classified outbound/crossbound DDoS attacks during the survey period. However, only 53 percent mitigated these attacks (Figure 18, page 16). We believe that this mitigation deficit is due in part to an almost exclusive focus on technical means for mitigating inbound attacks, along with a misperception that outbound/crossbound attacks are somehow less serious from an operational point of view.

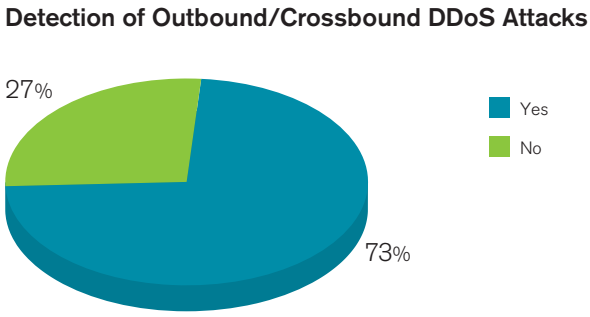

Figure 17
Source: Arbor Networks, Inc.

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.

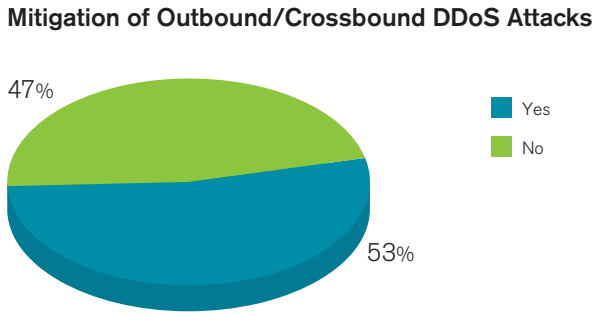

Figure 18
Source: Arbor Networks, Inc.

Attack Detection, Classification and Traceback

The composition of tools used to detect, classify and traceback DDoS attacks (Figure 19) generally corresponds to responses noted in the section of this report entitled *Scale, Targeting and Frequency of Attacks* (beginning on page 13), which identifies the tools used to detect and classify the single-largest DDoS attack experienced by respondents during the survey period (Figure 16, page 15). Again, commercial flow-telemetry collection/analysis systems were the most commonly used tool. However, more day-to-day emphasis has been placed by operators on in-house developed tools and commercial SNMP-based tools over open-source flow-telemetry collection/analysis systems.

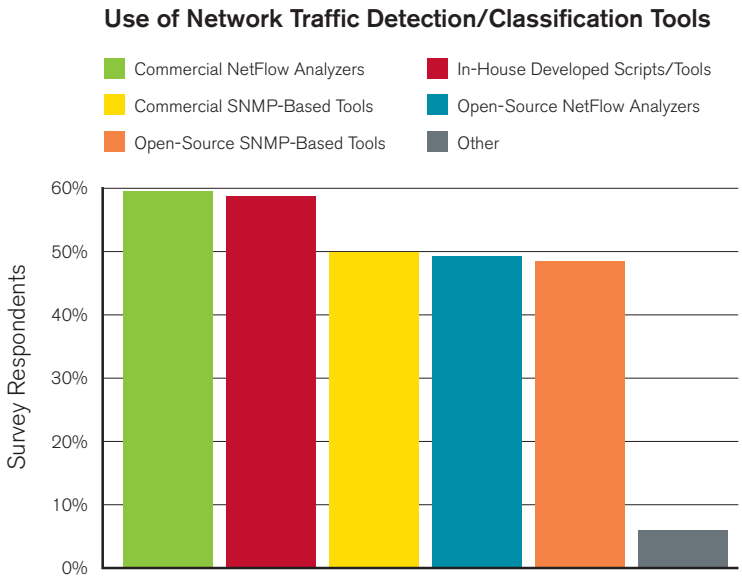

Figure 19
Source: Arbor Networks, Inc.

Other tools reported in use by respondents include IDS, syslog-based analysis systems, sinkholes, darknets, honeypots and NMS. One particularly poignant free-form response in this section read as follows:

> "No tools used today, sadly. Flying blind."

Figure 20 illustrates that while 47 percent of respondents indicate they do not employ event-correlation tools to assist in detecting and classifying DDoS attacks, 53 percent make use of either commercial, in-house developed or open-source correlation systems—a significant increase over previous years.

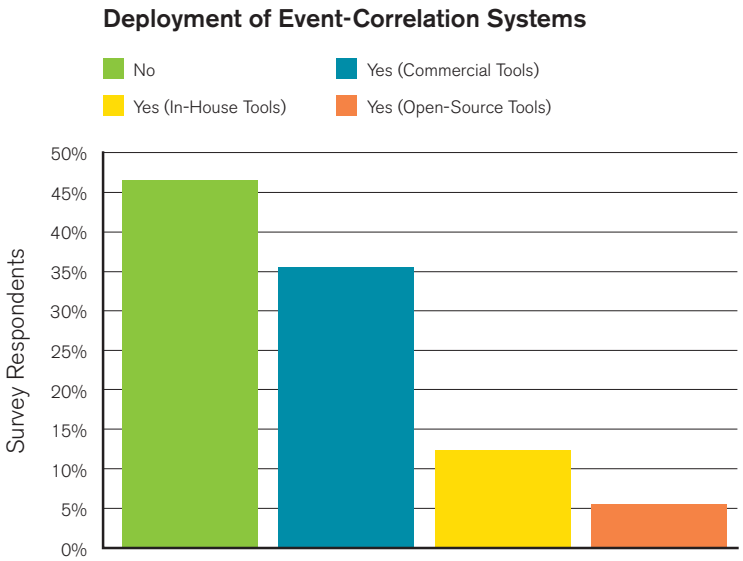

Figure 20
Source: Arbor Networks, Inc.

We believe that this apparent increase in the popularity of event-correlation systems among respondents is due in large part to the increased geographical diversity and broader organizational categorizations of this year's respondent pool as shown earlier in Figures 2 and 3 (page 7), and Figure 4 (page 8).

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 21). Intelligent DDoS mitigation systems (IDMS) such as the Arbor Peakflow SP Threat Management System ("TMS") and the now-discontinued Cisco Guard are the second most widely used mitigation mechanisms.

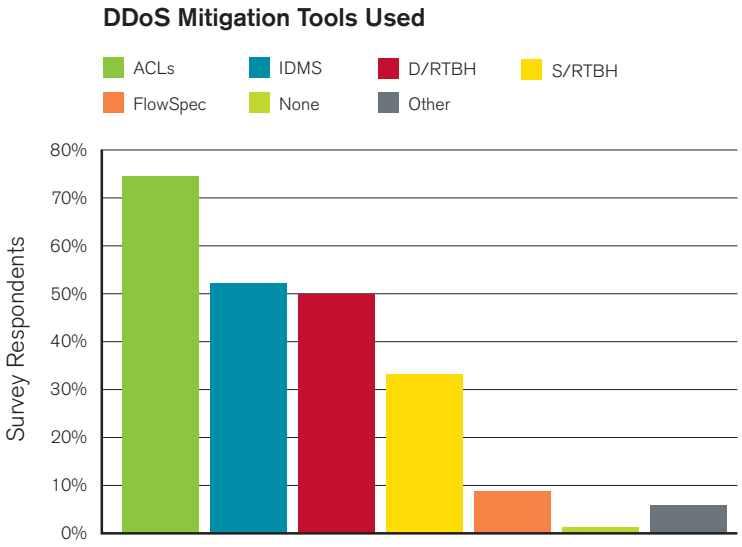

Figure 21
Source: Arbor Networks, Inc.

A full 50 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 for the attacker, penalizing the attack victim.

Other techniques utilized by respondents include custom-coded application-layer classification tools and GeoIP-based blocking of attack traffic purportedly emanating from specific geopolitical localities.

No respondents this year 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 programmatically generated attack traffic to "crowd out" traffic from legitimate sources.

Fifty-one percent of respondents indicated that they are able to successfully mitigate DDoS attacks within 20 minutes (Figure 22, page 19), a marked improvement over previous years. Fourteen percent indicated mitigation times in excess of 30 minutes, while another 14 percent reported that they mitigate attacks automatically, presumably in near real time.

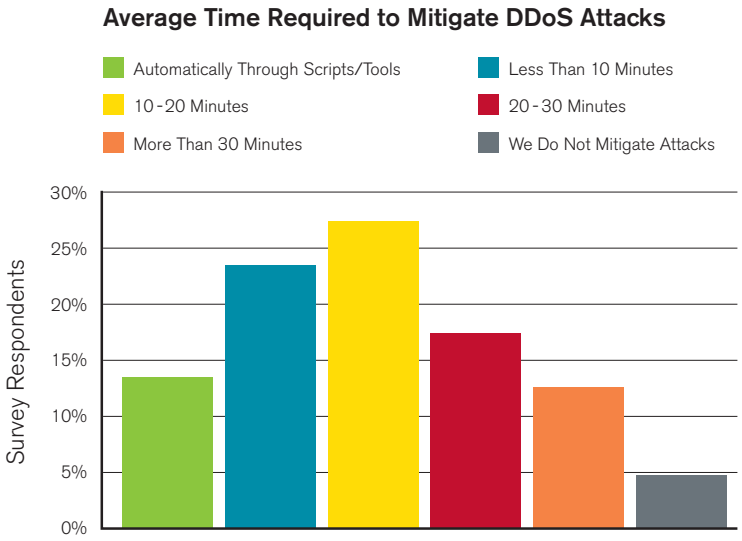

Figure 22
Source: Arbor Networks, Inc.

Focusing specifically on outbound/crossbound DDoS attacks (Figure 23), ACLs once again are the single most widely utilized tool to mitigate attack traffic. Thirty percent of respondents indicated that D/RTBH is used to mitigate outbound/crossbound attacks, again completing the DDoS for the attacker. Meanwhile, 28 percent indicated that they do not mitigate outbound/crossbound attacks at all.

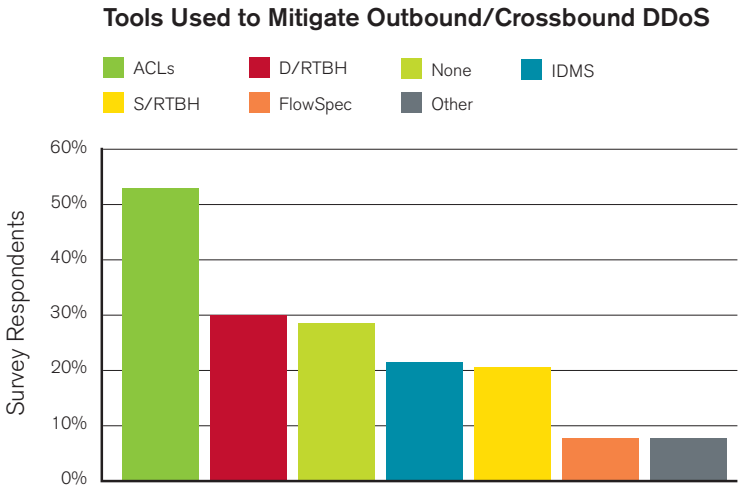

Figure 23
Source: Arbor Networks, Inc.

Other tools and techniques utilized to mitigate outbound/crossbound DDoS attacks include DNS blackholing (which also has the effect of completing the DDoS for the attacker) and QoS mechanisms (which are more suitable for mitigating outbound/crossbound attack traffic rather than inbound attacks toward servers, services and applications).

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 24). Thirty-four percent indicated that they do in fact attempt to block these undesirable hosts on a proactive basis.

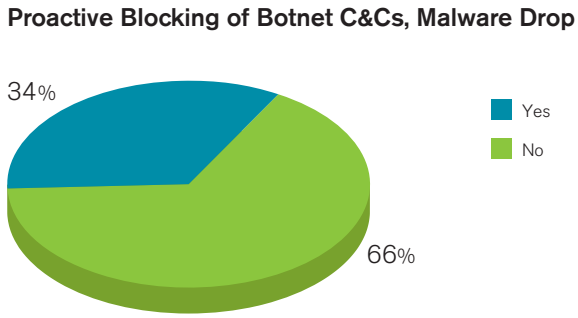

Figure 24
Source: Arbor Networks, Inc.

Managed Security Services

Forty-one percent of respondents indicated that they offer managed security services (Figure 25), with the most popular being managed router, managed VPN and traffic visibility services (Figure 26, page 21). Of this pool of respondents, 55 percent offer "Clean Pipes" managed DDoS mitigation services, tying with the percentage of those who offer managed firewall services, which has been one of the most popular managed security service offerings noted by respondents in previous surveys.

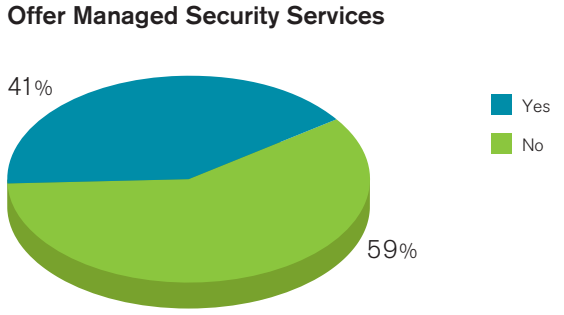

Figure 25
Source: Arbor Networks, Inc.

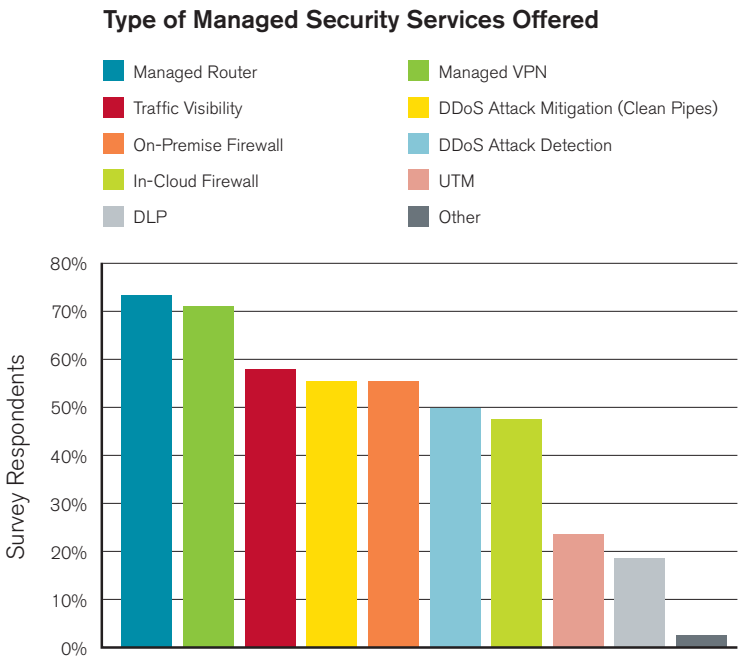

Figure 26
Source: Arbor Networks, Inc.

Of the respondents offering Clean Pipes managed DDoS mitigation services, 56 percent offer end customers the option of self-initiating DDoS mitigation (Figure 27), a significant increase over previous reports. This increase in self-mitigation availability 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.

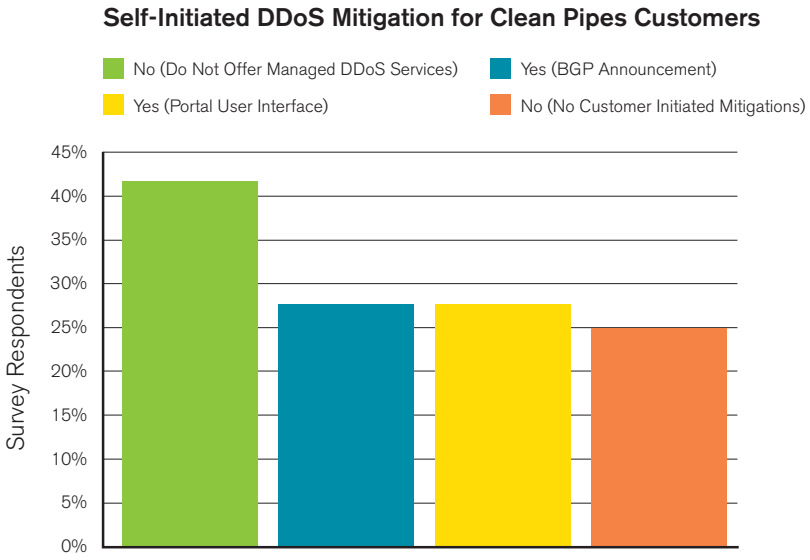

Figure 27
Source: Arbor Networks, Inc.

Respondents offering managed security services reported a small head count of dedicated managed security services personnel, with only 16 percent employing more than 10 dedicated staff members (Figure 28).

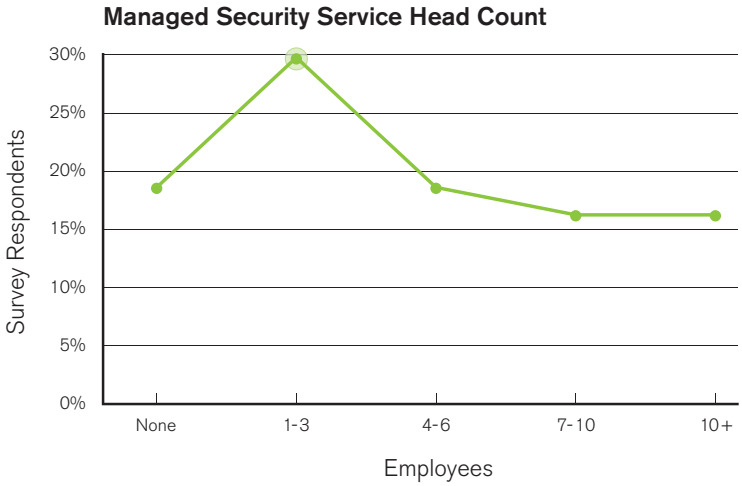

Figure 28
Source: Arbor Networks, Inc.

Observations on Operational Security Groups, Law Enforcement, CERTs and CSIRTs

Figures 29 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.

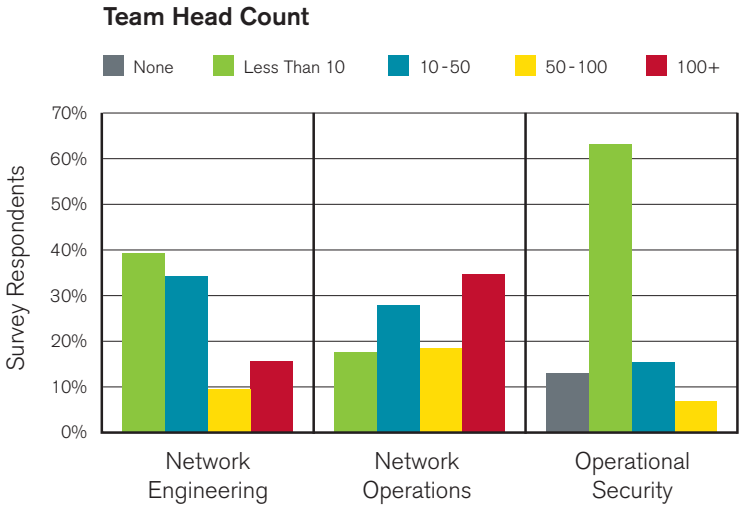

Figure 29
Source: Arbor Networks, Inc.

As in previous reports, lack of head count and/or resources topped the list of operational security challenges faced by respondents (Figure 30). 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. The most salient comment in this section follows:

> "It's not seen as revenue generating, so it's not a profit center, [so] no support. Stupid."

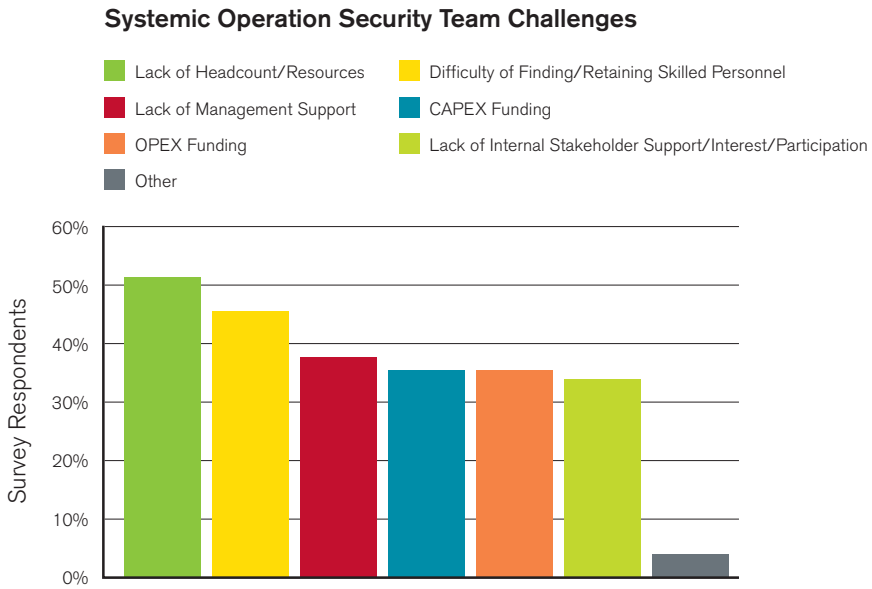

Figure 30
Source: Arbor Networks, Inc.

Figures 31 (below) and 32 (page 24) illustrate that while 88 percent of respondent organizations operate a NOC, only 36 percent operate a SOC.

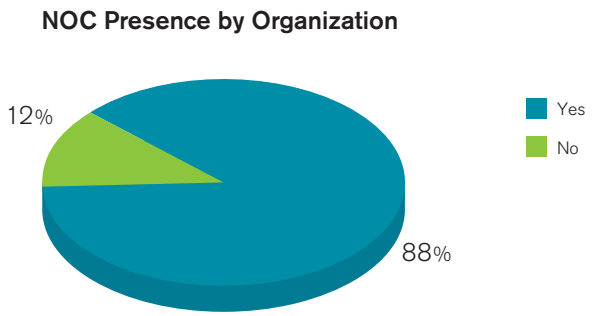

Figure 31
Source: Arbor Networks, Inc.

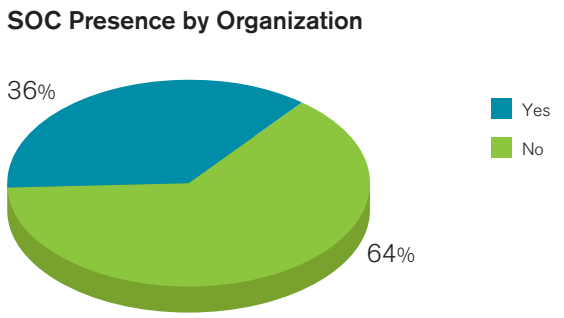

Figure 32
Source: Arbor Networks, Inc.

Given the aforementioned SOC deficit (Figure 32), it is unsurprising to note that 72 percent of respondent organizations never rehearse their operational security plans and procedures or conduct OPSEC drills (Figure 33). One notable comment from this section follows:

> "Practice? You mean, simulate an attack against our own test infrastructure? It's against AUP, so we don't even permit/ suggest that our customers do this."

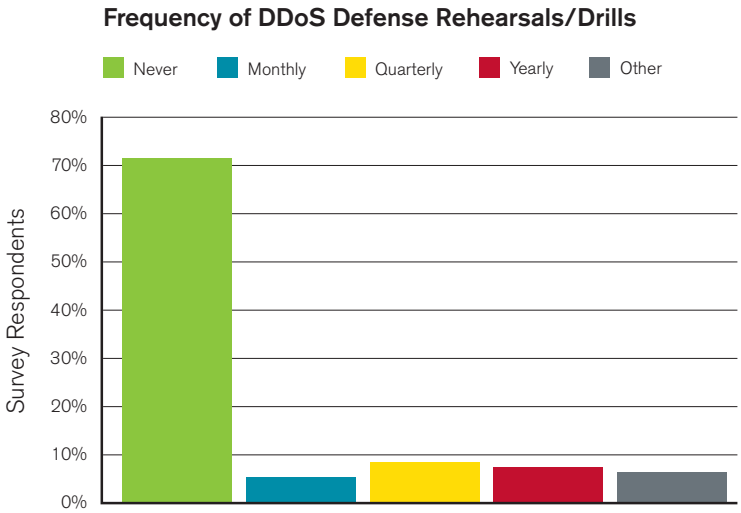

Figure 33
Source: Arbor Networks, Inc.

On a more positive note, 78 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 elements of their peers, transit providers and customers (Figure 34).

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

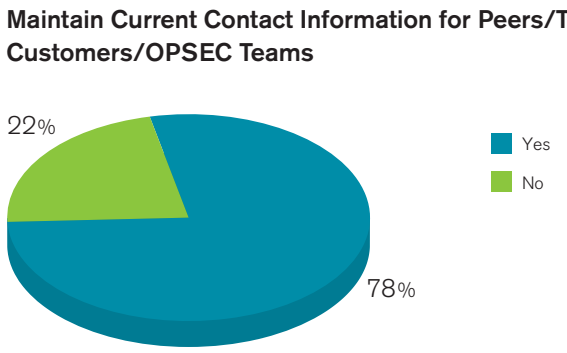

Figure 34
Source: Arbor Networks, Inc.

Security-related email lists remain the single most popular way of staying aware of relevant security information from outside sources (Figure 35). Other popular methods reported by this year's respondents include industry conferences, vendor-specific email lists and weblogs. Social media such as Twitter and Facebook are increasing in popularity for this application, with nearly one-third of respondents making use of these tools to garner operationally relevant information. Other primary sources of security-related information utilized by respondents include closed or vetted operational security groups, FIRST, and various CERT and CSIRT organizations.

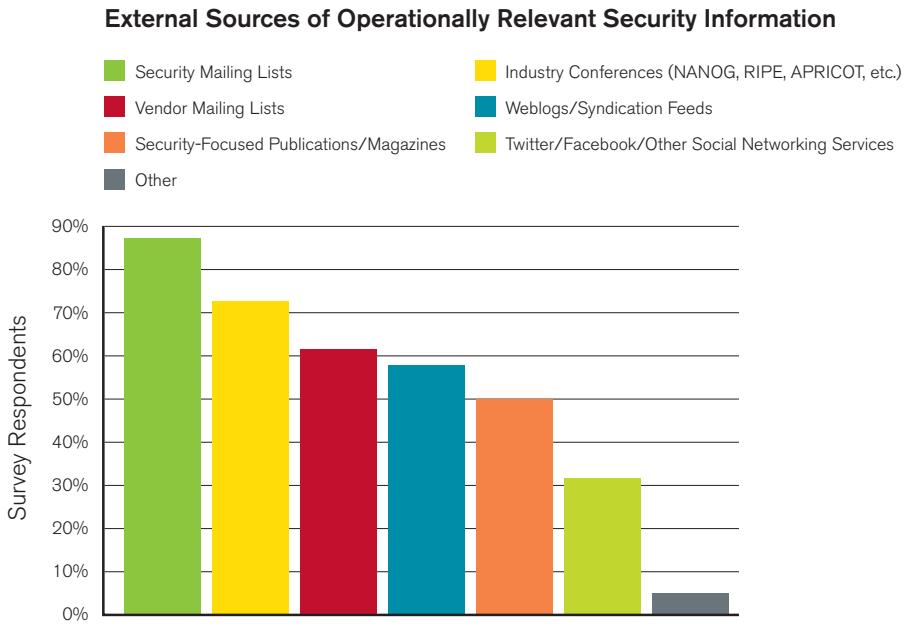

Figure 35
Source: Arbor Networks, Inc.

Only 40 percent of respondents indicated that they participate in closed or vetted global operational security groups (Figure 36), while 88 percent indicated that they believe these groups are highly effective in handling operational security issues on an interorganizational basis (Figure 37). One detailed free-form comment follows:

> "Most of these groups all come with some form of 'baggage.' Many of the so-called trust groups are as distrustful of each other as they are of the real bad actors, making these groups much less useful than they should be. They're all good to help build direct relationships, which often take over after the groups have served their initial purpose and decay in trust or usefulness sets in."

Participation in Vetted Operational Security Groups/Systems

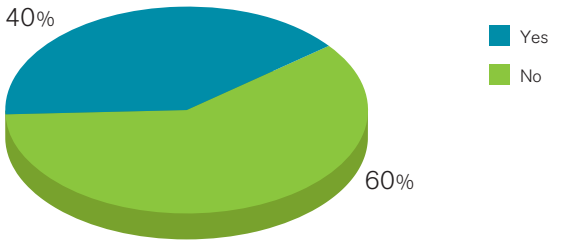

Figure 36
Source: Arbor Networks, Inc.

Confidence in Efficacy of Vetted Operational Security Groups/Systems

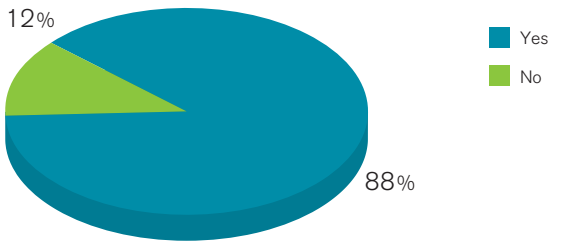

Figure 37
Source: Arbor Networks, Inc.

As with OPSEC teams in general, significant systemic challenges to full participation in closed/vetted global OPSEC groups persist (Figure 38). Lack of time/resources is the most frequently cited challenge, along with lack of management support, policy barriers, unclear benefits and concerns around participant vetting. Respondents also cited legal concerns, along with additional challenges, as noted below:

> "Internal political considerations."

> "We're very active participants, but some things are not sent to these trust groups for a variety of reasons, including some of the challenges listed above. Additionally, many players in these groups seem to leverage or bend any success of these groups to their own personal or commercial advantage."

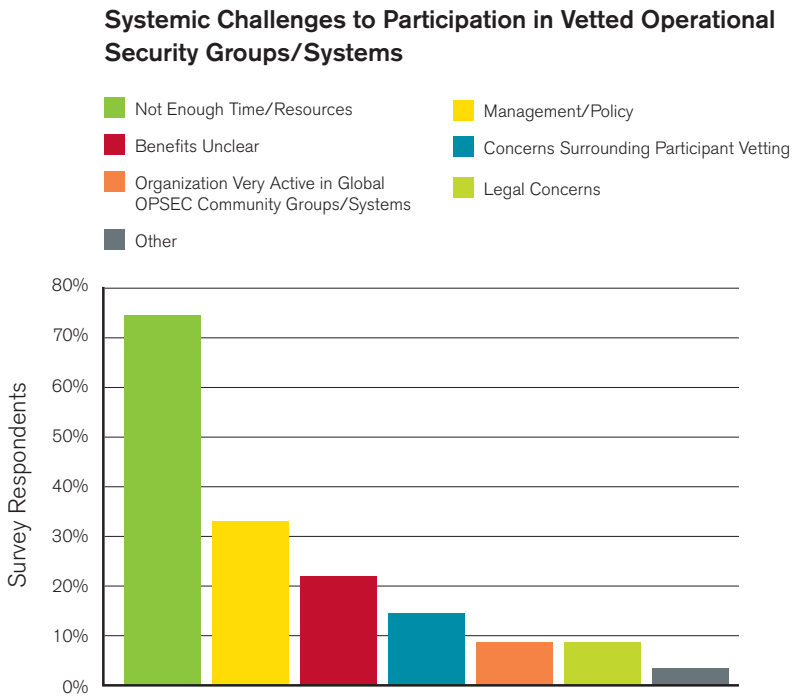

Figure 38
Source: Arbor Networks, Inc.

Sixty-one percent of respondents indicated that they do not refer security incidents to law enforcement (Figure 39). 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 40).

Free-form comments from respondents who do not currently make law enforcement referrals follow:

> "Lack of cross-jurisdictional support for investigations. In the end, they go nowhere."
> "FCC rules prevent sharing customer data—plus, how effective would it be? :("
> "I'm not at liberty to answer."

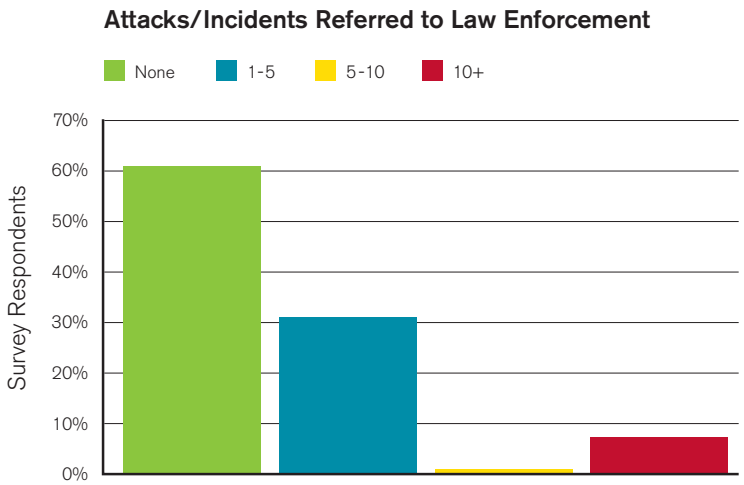

Figure 39
Source: Arbor Networks, Inc.

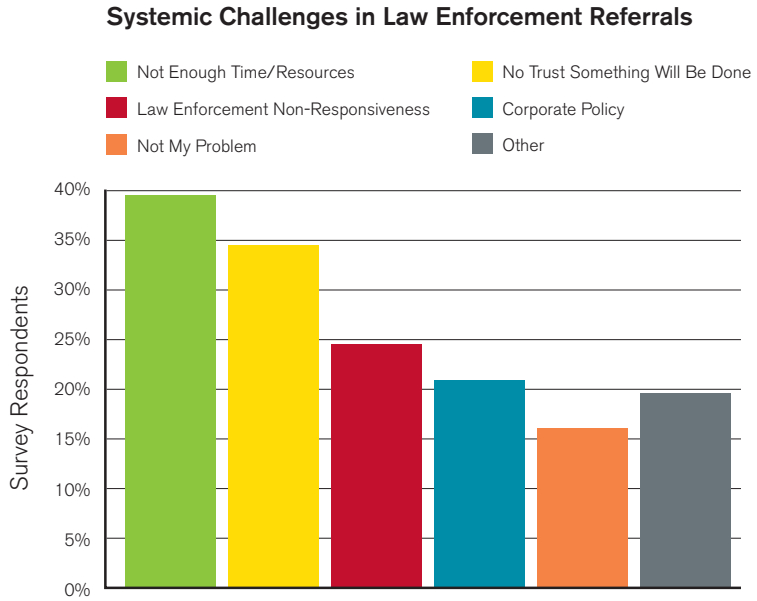

Figure 40
Source: Arbor Networks, Inc.

Overall, confidence in law enforcement efficacy is quite low (Figure 41). A large plurality of respondents see no evidence of positive change in law enforcement efficacy year over year (Figure 42).

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, prosecution and incarceration of Internet criminals.

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.

Confidence in Law Enforcement Investigative Efficacy

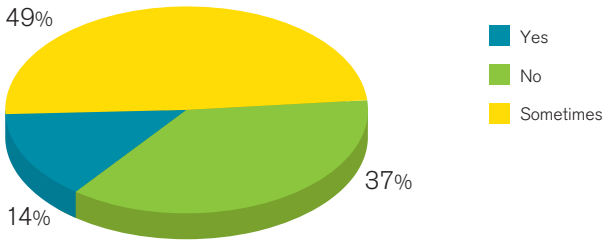

Figure 41
Source: Arbor Networks, Inc.

Perceived Changes in Law Enforcement Investigative Efficacy

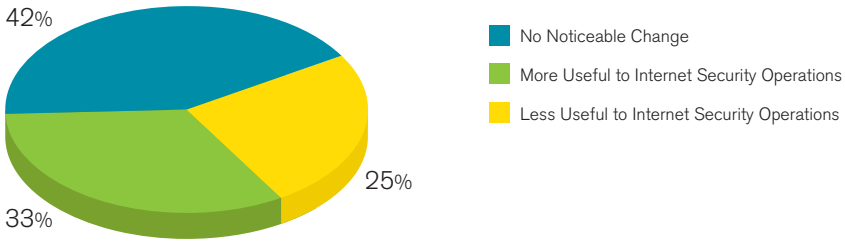

Figure 42
Source: Arbor Networks, Inc.

Figures 43 and 44 illustrate that 37 percent of respondent organizations have established an internal CERT, and 70 percent are actively engaged with their respective national or regional CERTs and/or CSIRTs.

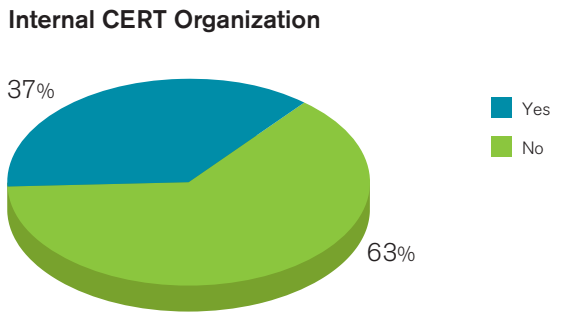

Figure 43
Source: Arbor Networks, Inc.

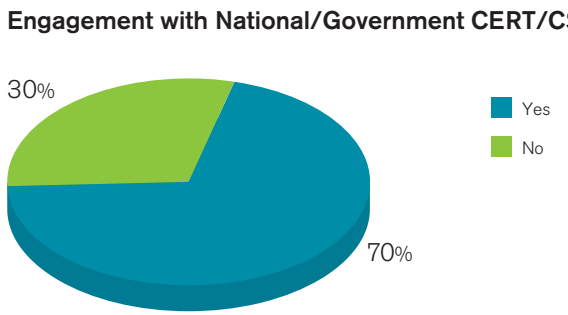

Figure 44
Source: Arbor Networks, Inc.

Furthermore, 86 percent of respondents believe that government CERTs/CSIRTs have a positive role to play in operational security incident response and welcome their involvement (Figure 45). 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.

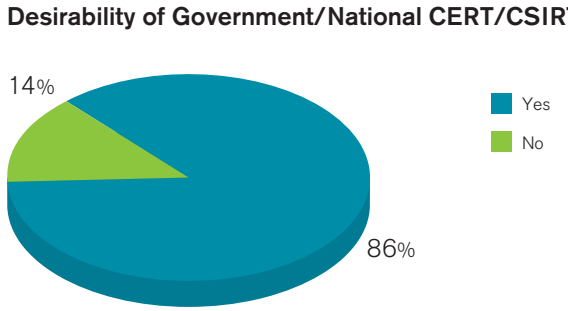

Figure 45
Source: Arbor Networks, Inc.

In contrast with their expressed positive view of national or regional CERT/CSIRT engagement, 75 percent of respondents have a negative view of government efforts in the area of critical infrastructure protection (Figure 46).

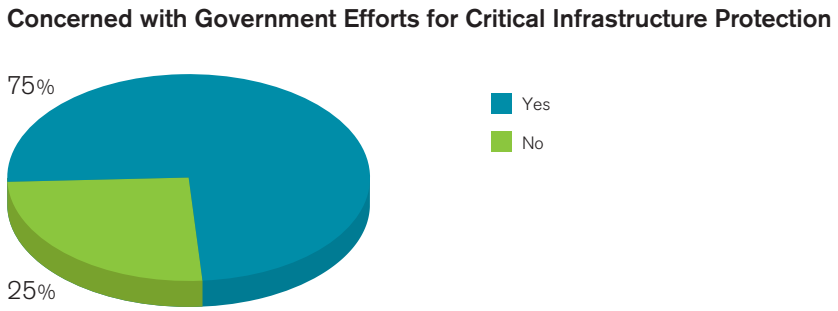

Figure 46
Source: Arbor Networks, Inc.

Infrastructure Protection Techniques

Figure 47 illustrates that a majority of respondent organizations have implemented 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. Forty-four percent perform IRR registration of their customer routes.

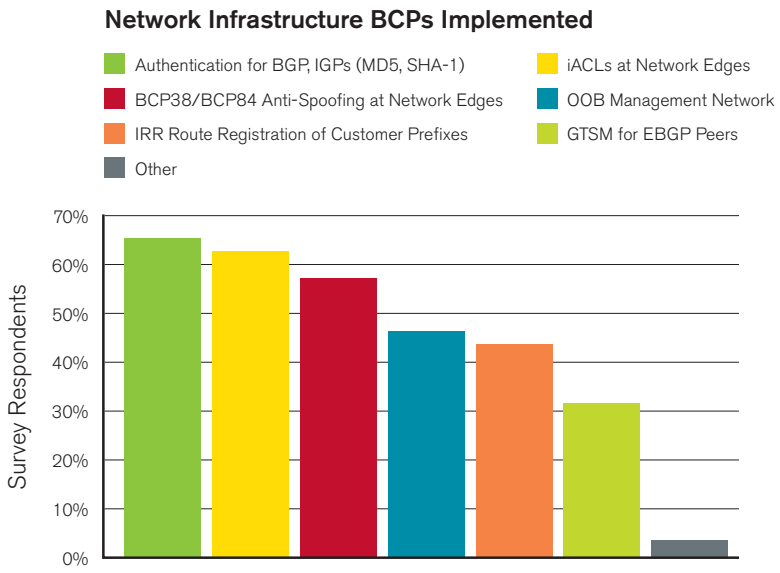

Figure 47
Source: Arbor Networks, Inc.

Based on survey response, 70 percent of IDC operators have implemented various Layer 2 BCPs (Figure 48). 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.

Layer 2 Infrastructure BCPs Deployed in IDC Environments

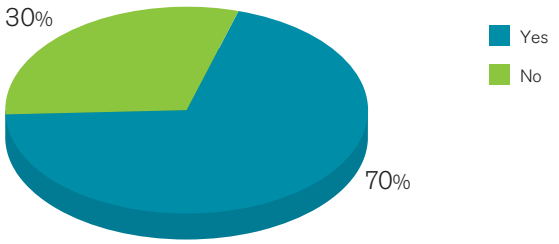

Figure 48
Source: Arbor Networks, Inc.

Similar good news exists on the route-filtering front, with 81 percent of respondent organizations explicitly filtering customer route announcements (Figure 49).

Explicit Filtering of Customer Routing Advertisements

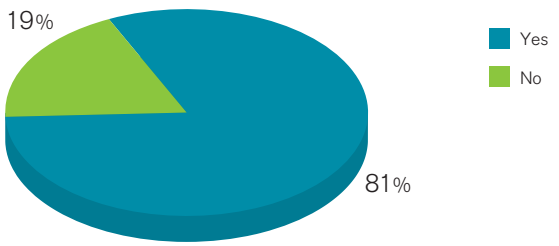

Figure 49
Source: Arbor Networks, Inc.

Meanwhile, only 57 percent of respondents explicitly filter inbound routing advertisements from peers and upstream transit providers (Figure 50).

Explicit Filtering of Inbound Peer/Upstream Routing Advertisements

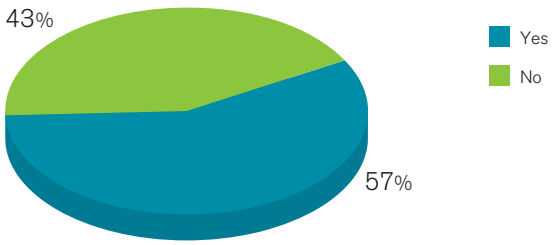

Figure 50
Source: Arbor Networks, Inc.

IPv6 Observations

In the 2009 *Worldwide Infrastructure Security Report,* we highlighted IPv4 address depletion and the necessity of deploying IPv6 as two major challenges facing service providers in 2010; this prediction is largely borne out by responses to this year's survey, which indicate serious concerns regarding visibility and control parity of IPv6-enabled networks with IPv4 networks.

Fifty-six percent of respondents indicated that they believe IPv4 address allocations will not prove to be a serious problem during the next 12 months (Figure 51). We're unsure as to whether this majority view is indicative of extreme confidence in forthcoming IPv6 deployments (an unlikely interpretation, given answers to subsequent survey questions regarding IPv6); 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 CGNs will be sufficient in the medium term for addressing end-customer needs.

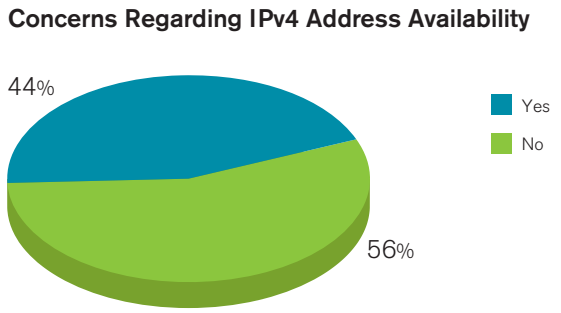

Figure 51
Source: Arbor Networks, Inc.

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

> "Allocations might be a problem for someone in the next 12 months, but not me. It might be a problem a few years from now."

> "IPv4 depletion is coming in the next year; it's possible we could end up with an upsurge in clients needing address space, and will not be able to get it."

> "Unsure how many future allocations from APNIC we will get. If we do not get any more, we might be able to survive for about 12 months before implementing IPv6 for all customers (difficult) or performing some CGN (presents port and billing issues)."

> "We ran out of public space in one of our IDCs 2 weeks ago. We have more address space, but it's going to require some re-engineering to make usable."

> "Already overusing our allocation; indications are we won't be able to get sufficient numbers of additional addresses to support existing services. Heavy use of PAT already underway."

Sixty-four percent of respondents stated that their production network infrastructure currently supports IPv6 today (Figure 52), while an additional 13 percent indicated that they plan to implement production support within the next 12 months (77 percent cumulative, Figure 53).

IPv6 Currently Implemented on Network Infrastructure

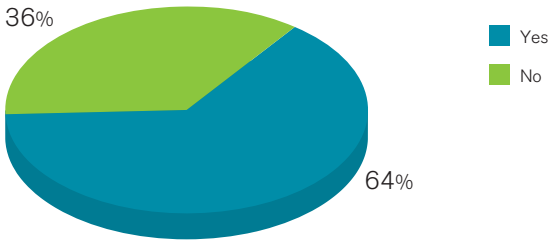

Figure 52
Source: Arbor Networks, Inc.

IPv6 Deployed Currently or Within Next 12 Months

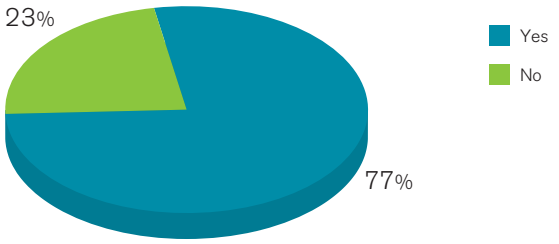

Figure 53
Source: Arbor Networks, Inc.

Forty-eight percent of respondents indicated that they are already 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 54).

IPv6 Used for Infrastructure Addressing

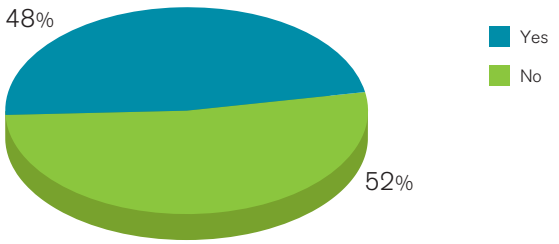

Figure 54
Source: Arbor Networks, Inc.

Figure 55 summarizes that 79 percent of respondents view visibility into IPv6 traffic on their networks as critical. Figure 56 illustrates that 41 percent indicated full network infrastructure vendor support for IPv6 flow telemetry today, and 34 percent indicated their current network infrastructure offers at least partial support for IPv6 flow telemetry.

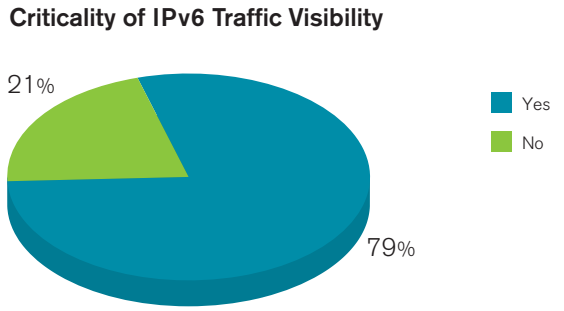

Figure 55
Source: Arbor Networks, Inc.

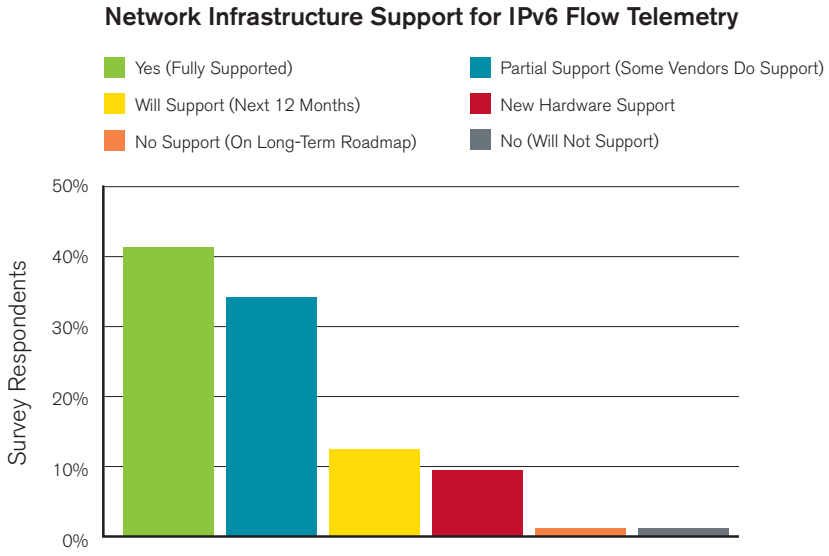

Figure 56
Source: Arbor Networks, Inc.

While 33 percent of respondents project that their IPv6 traffic volume will increase 20 percent over the next 12 months, 29 percent forecast greater than a 100 percent IPv6 volume increase over the same period (Figure 57).

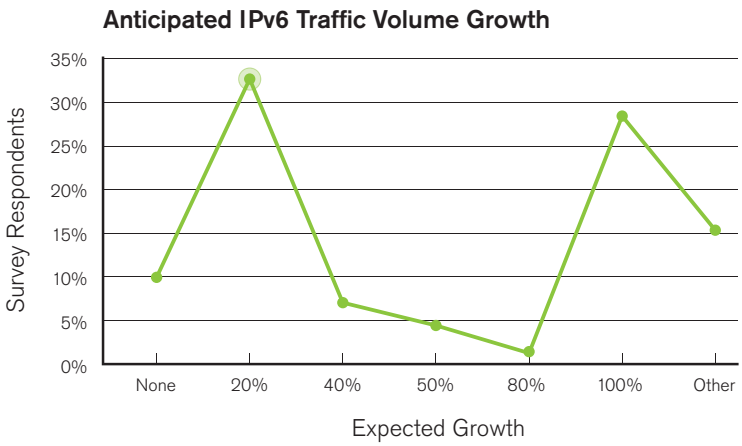

Figure 57
Source: Arbor Networks, Inc.

Figure 58 summarizes that 57 percent of respondents stated that misconfigurations resulting in outages are their foremost security concern related to IPv6. Fifty-five 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. Forty-seven percent expressed concern regarding IPv6 DDoS attacks, with a similar proportion expressing concern regarding IPv6 stack implementation flaws that may lead to security vulnerabilities in their network infrastructure elements.

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

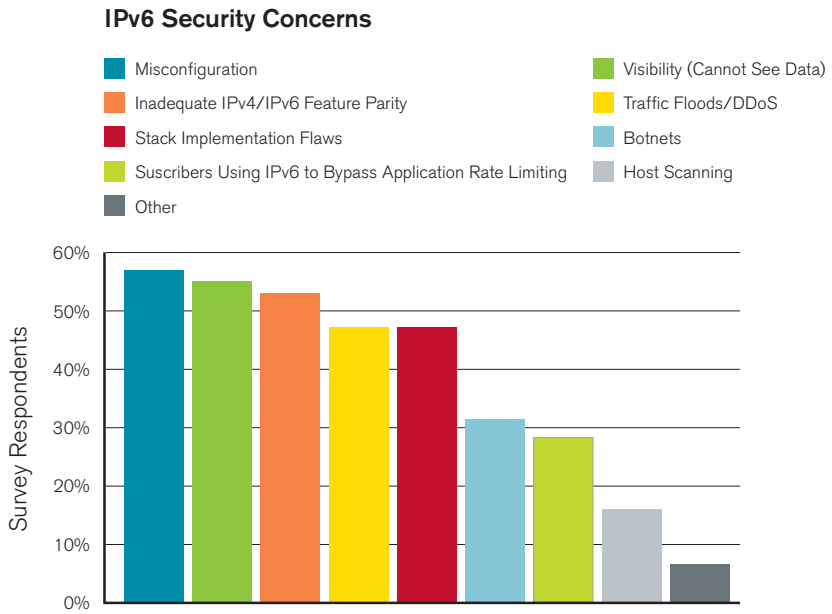

Figure 58
Source: Arbor Networks, Inc.

Despite the previously mentioned limitations of ACLs, 60 percent of respondents reported that they use or intend to use such lists to mitigate IPv6 DDoS attacks (Figure 59). Thirty-nine percent stated that they use or intend to use IDMS. Thirty-seven 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.

Twenty-one 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.

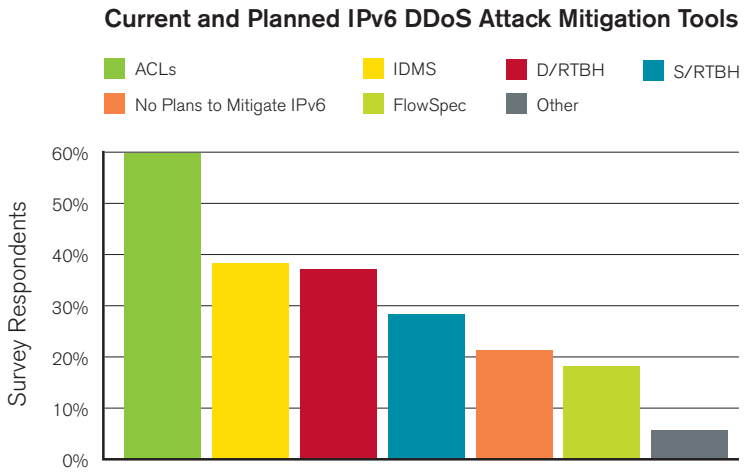

Figure 59
Source: Arbor Networks, Inc.

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. Operators should 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 a historical note, the first IPv6-related DDoS attack of which Arbor personnel are aware took place in 2004. The target was the 6-to-4 gateway of a major EMEA-based network operator. This gateway was being attacked from the IPv4 Internet, and a relatively small amount of traffic was all that was required to bring it down—disrupting service for all legitimate users of the gateway.

It was determined that this attack was the result of a feud between rival botmasters. The attacker's intention was to obstruct the IPv6-encapsulated and obfuscated botnet C&C traffic of his opponent by taking down the 6-to-4 gateway in question.

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 network resilience.

IDC Operator Observations

Figure 60 illustrates that 74 percent of respondents operate IDCs. Of those respondents, 69 percent indicated they had experienced DDoS attacks directed at targets within their IDCs during the 12-month survey period (Figure 61).

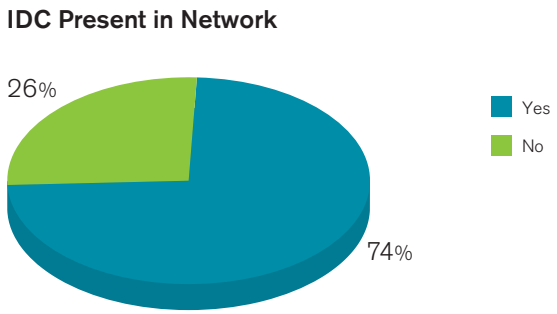

Figure 60
Source: Arbor Networks, Inc.

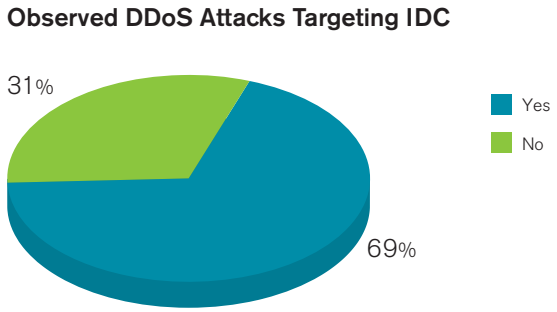

Figure 61
Source: Arbor Networks, Inc.

With regards to application-layer DDoS attacks targeted at servers, services and applications residing within IDCs, 78 percent of respondents experienced HTTP DDoS attacks during the survey period (Figure 62). Sixty-five percent experienced DNS-focused DDoS attacks, while 35 percent experienced SMTP-directed DDoS attacks. VoIP systems, gaming servers and, again, TCP port 123 were also listed as application-layer attack targets.

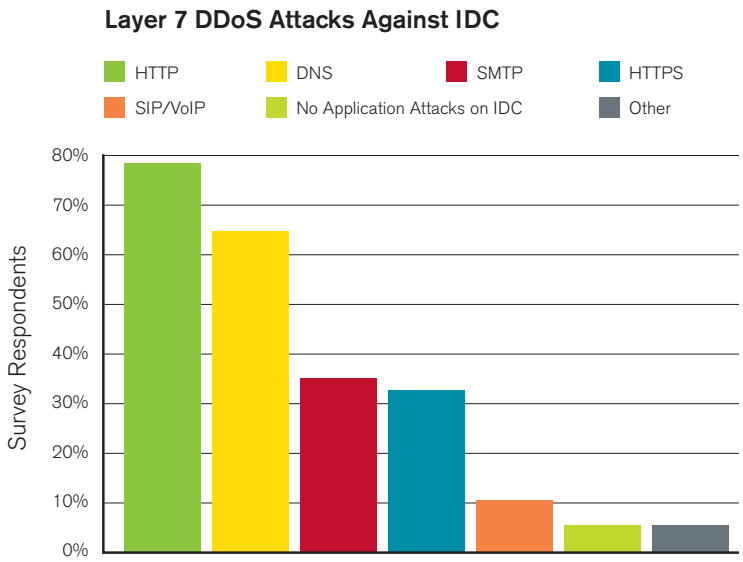

Figure 62
Source: Arbor Networks, Inc.

Figure 63 illustrates that only 15 percent of respondents experienced a DDoS attack that exceeded the uplink capacity from their IDC to their core network and/or peering/transit providers during the survey period. We believe that this is directly related to the brittleness of the application, server or service architectures, as well as network architectural flaws. In many cases, these deficiencies would substantially reduce the need for attackers to utilize large amounts of bandwidth to negatively impact the availability of DDoS targets residing within the IDC. Lower-bandwidth, application-layer attacks focused on exposing the limitations of the IDC 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.

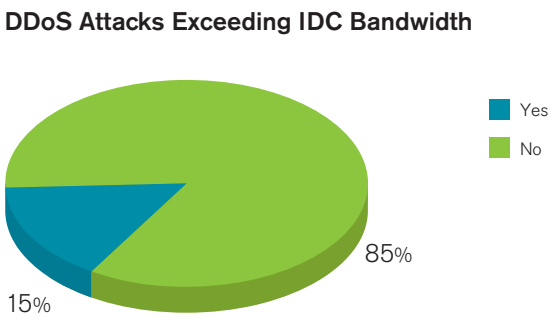

Figure 63
Source: Arbor Networks, Inc.

It may be tempting to speculate that increases in link bandwidth may also account for the relatively low number of IDC operators who have experienced link-filling attacks. However, it is important to remember that, in an era of 100 Gbps DDoS attacks, attackers have the ability to overwhelm link bandwidth at will. In most (not all) cases, attackers tend to utilize only the amount of attack resources necessary to accomplish their goals. Due to the aforementioned brittleness and fragility of many applications and services, attackers generally do not need to engage in link-flooding attacks against IDC targets to accomplish their goal of service disruption.

Finally, many DDoS attacks are not directly launched by the instigators of the attacks. Instead, they pay botmasters to launch the attacks. The fee scale for doing so often includes a bandwidth component. Even if they are paying with stolen credit cards or other fraudulently obtained means, which is often the case, the instigators of attacks do not wish to spend more than is necessary to accomplish their goals.

The data represented in Figure 64 emphasizes the fact that the attack surface of the IDC includes both the underlying services and service architecture, as well as the network-level architecture and capacity. Seventy percent of respondents who operate an IDC indicated that they experienced DDoS attacks directed at ancillary IDC services such as Web portals, shared Web hosts, DNS servers and SMTP servers during the survey period.

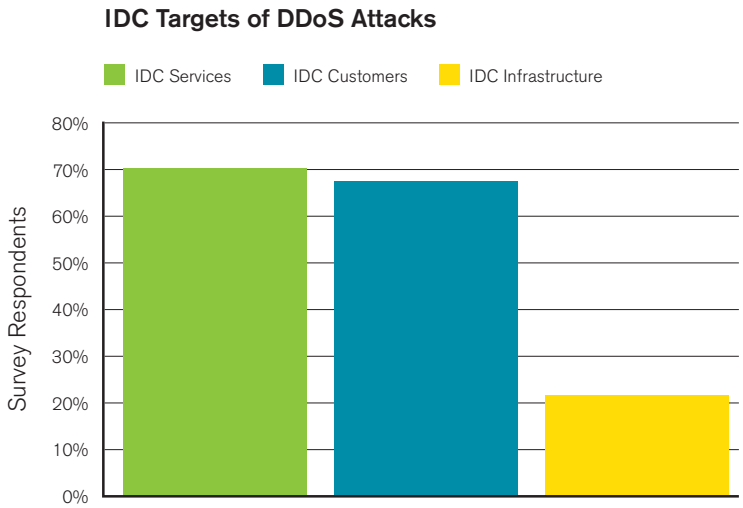

Figure 64
Source: Arbor Networks, Inc.

Twenty-seven percent noted that they experienced between 1 and 10 IDC-targeted DDoS attacks per month during this survey period; an aggregate of 43 percent indicated they experienced between 10 and 500 DDoS attacks directed at their IDCs per month; and a small minority of 3 percent experienced more than 500 IDC-targeted DDoS attacks per month (Figure 65, page 41).

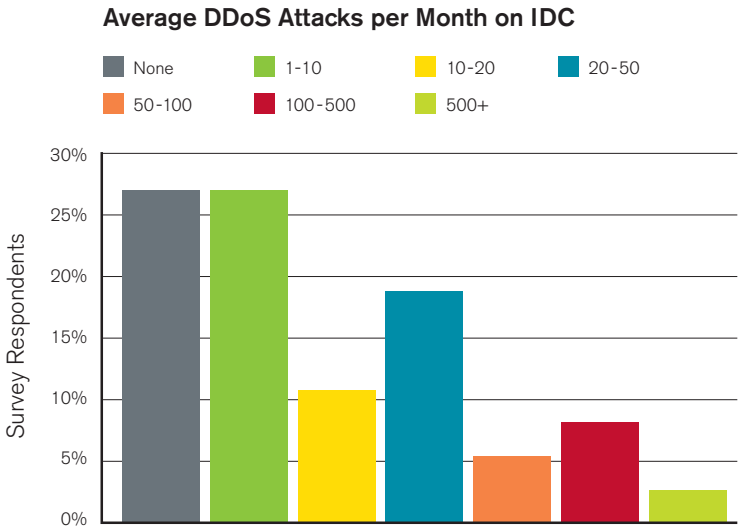

Figure 65
Source: Arbor Networks, Inc.

Figure 66 depicts that 84 percent of respondents experienced increased OPEX-related expenditures as a result of IDC-targeted DDoS attacks during the survey period, while 43 percent experienced customer churn and related revenue loss due to these attacks.

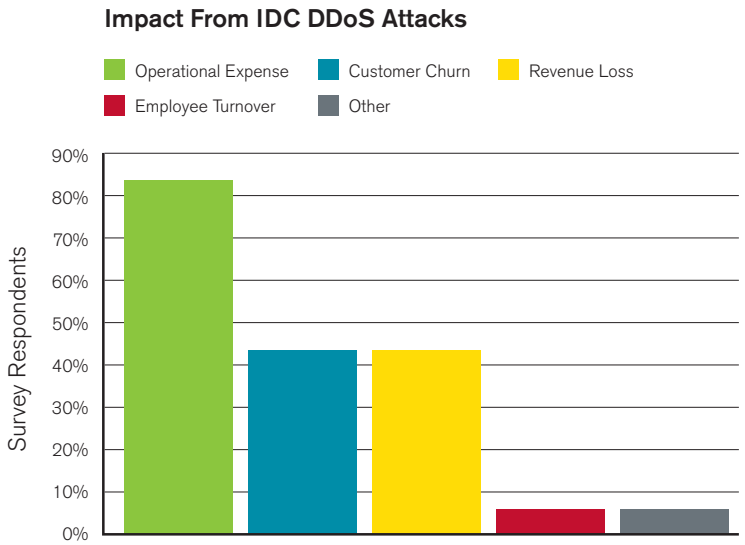

Figure 66
Source: Arbor Networks, Inc.

Eighty-six percent of respondents indicated that they or their customers have placed stateful firewall and/or IPS devices in their IDCs. Nearly half of all respondents—a solid majority of those who actually have deployed these devices within their IDCs—experienced stateful firewall and/or IPS failure as a direct result of DDoS attacks during the survey period. Only 14 percent indicated that they follow the IDC BCP of enforcing access policy via stateless ACLs deployed on hardware-based routers/Layer 3 switches capable of handling millions of packets per second.

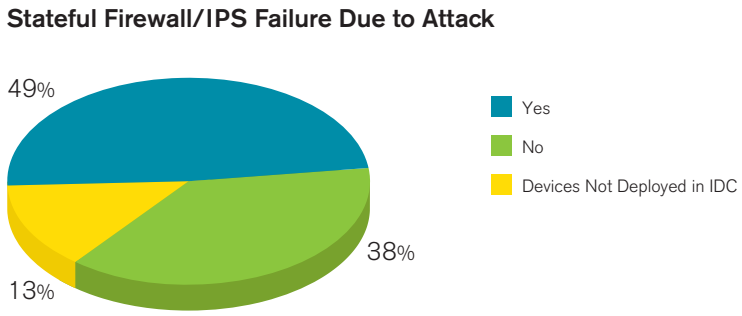

Figure 67
Source: Arbor Networks, Inc.

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.

Respondents listed ACLs as a primary mechanism for mitigating DDoS attacks against IDCs (Figure 68). They also identified stateful firewall and IPS devices as primary DDoS defense mechanisms. Forty-eight percent of respondents indicated that they make use of IDMS to mitigate IDC-targeted DDoS attacks, and 18 percent employ S/RTBH within their IDC environments.

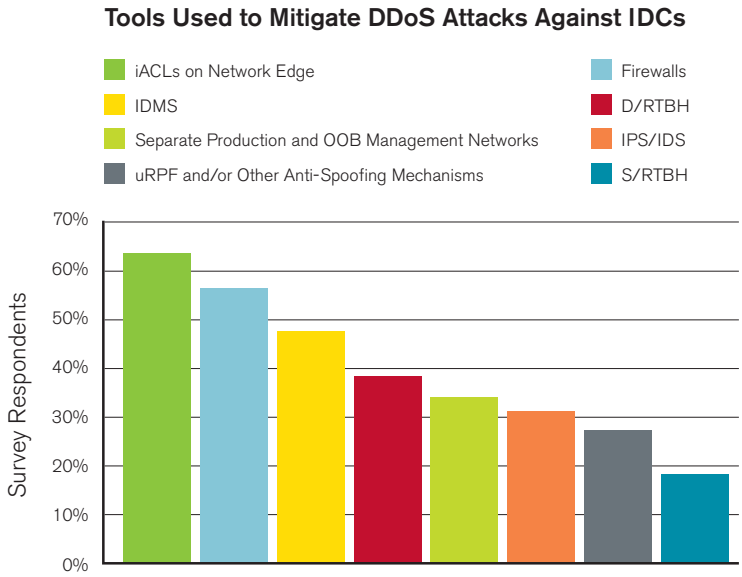

Figure 68
Source: Arbor Networks, Inc.

Mobile and Fixed Wireless Operator Observations

As indicated in Figures 69 and 70, 30 percent of respondents operate a mobile or fixed wireless network; in aggregate, 50 percent of those respondents serve anywhere from five million subscribers to more than 100 million subscribers on their wireless networks.

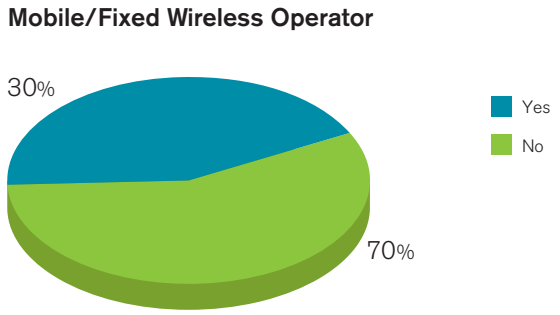

Figure 69
Source: Arbor Networks, Inc.

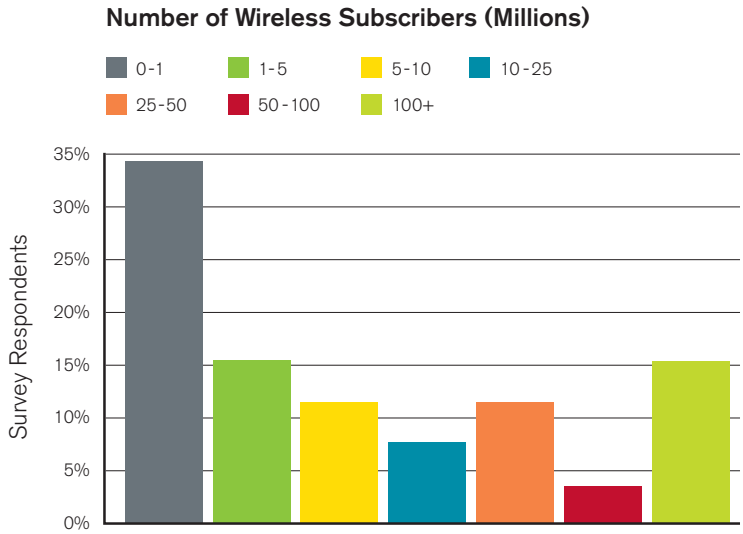

Figure 70
Source: Arbor Networks, Inc.

Respondents who operate mobile wireless networks reported approximately 8 GGSNs or HAs, 150 SGSNs or PDNs, and an average of 15 roaming partners on their networks (Figure 71).

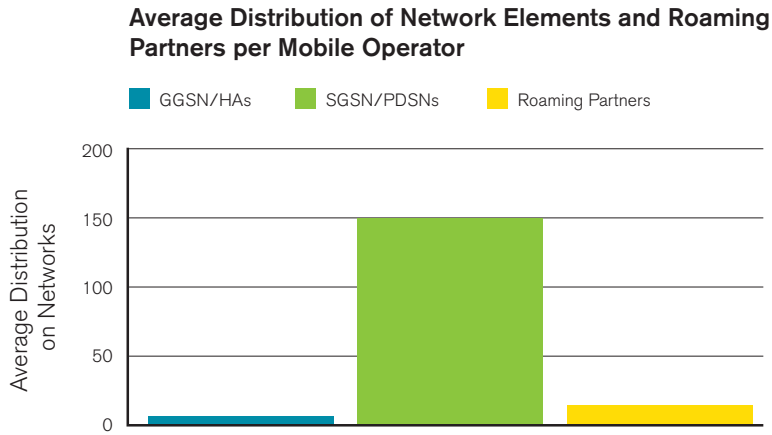

Figure 71
Source: Arbor Networks, Inc.

According to the data in Figure 72, some 65 percent of respondents have deployed 2G and/or 3G networks, 17 percent operate WiMAX networks and 9 percent operate LTE networks. The remainder operate WiFi hotspot networks or self-identify as MVNOs.

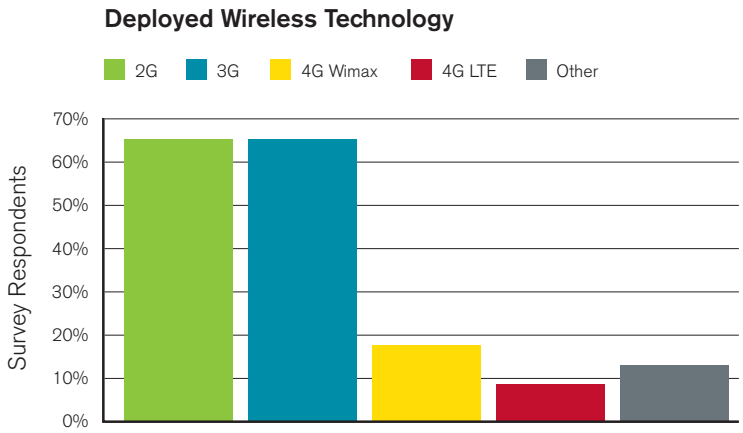

Figure 72
Source: Arbor Networks, Inc.

Among respondents yet to deploy 4G technologies, 52 percent indicate that they will deploy 4G technologies in 2014 or later, or whenever sufficient ROI has been achieved on their existing 2G/3G networks, whichever comes first (Figure 73).

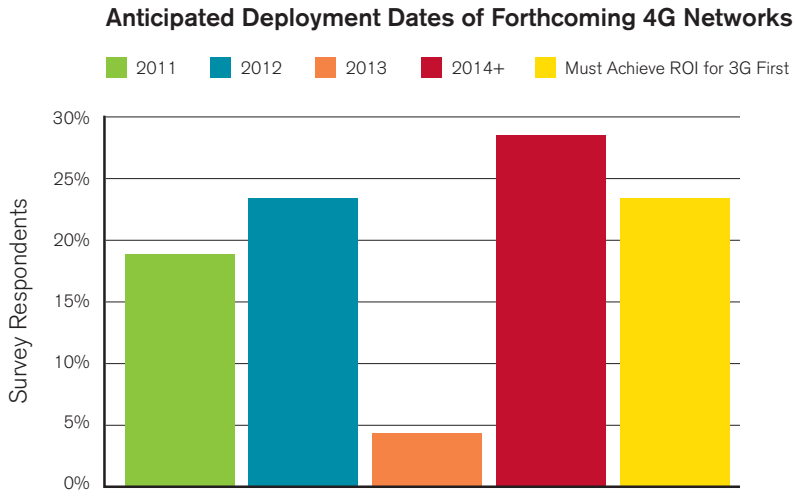

Figure 73
Source: Arbor Networks, Inc.

In terms of visibility into the network traffic of their wireless packet cores and their ability to classify core traffic as potentially harmful, 59 percent of respondents indicated they have limited or no visibility whatsoever (Figure 74). Only 23 percent indicated they have visibility into their wireless packet cores on par with or better than their visibility into their wireline packet cores.

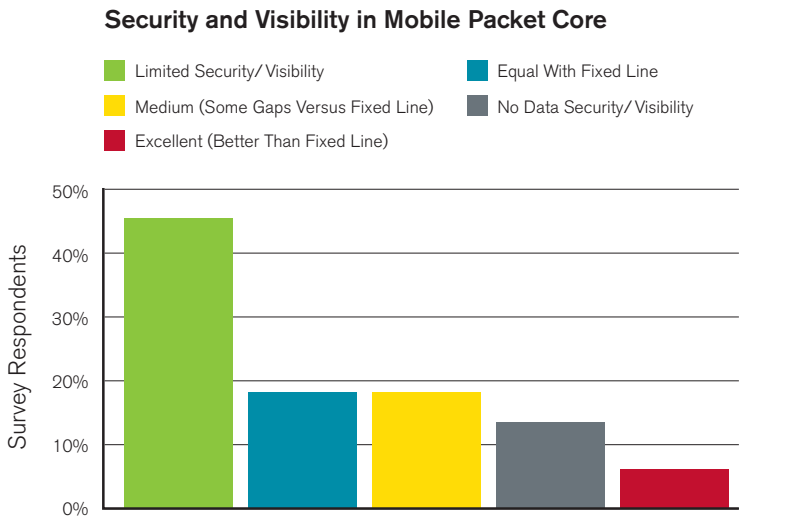

Figure 74
Source: Arbor Networks, Inc.

Of mobile wireless operator respondents, over 50 percent indicated that they have no visibility or extremely limited visibility into their network traffic at the Gi interface (Figure 75).

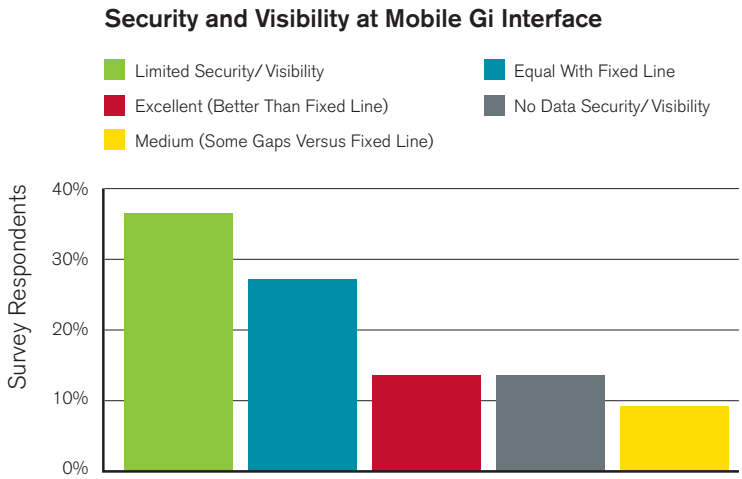

Figure 75
Source: Arbor Networks, Inc.

Seventy-nine percent of respondents believe that they have suffered no direct attacks on their wireless-specific network infrastructure within the 12-month survey period (Figure 76). However, accurate attack detection and classification is often problematic due to the limited network visibility highlighted above.

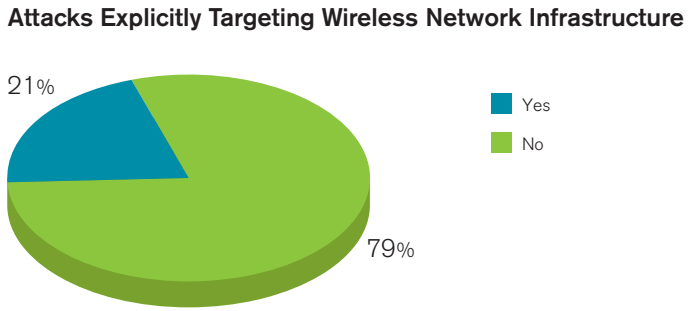

Figure 76
Source: Arbor Networks, Inc.

Forty-six percent of respondents stated that they have experienced visible customer outages during the survey period due to security incidents on their networks (Figure 77). Based upon the previously mentioned deficits in network visibility, we believe that this number may be under-reported as well.

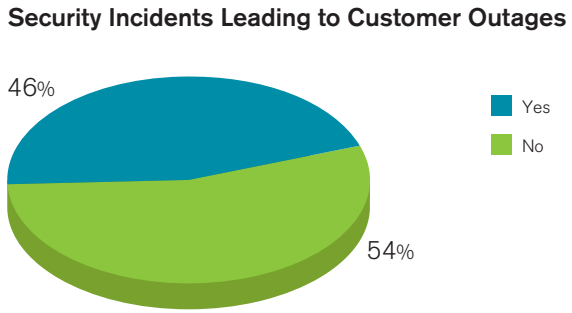

Figure 77
Source: Arbor Networks, Inc.

As illustrated in Figure 78, 56 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-four percent indicated that mobile handsets or end-customer computers with wireless connectivity have been affected by DDoS attacks. Significant proportions of the respondent base also stated that their data and signaling gateways, RANs and wireless packet core infrastructure have been affected by DDoS attacks.

Some 22 percent of respondents indicated that stateful firewalls and/or stateful NAT devices on their networks have been adversely affected by DDoS attacks during this period. As mentioned in the *IDC Operator Observations* section (pages 38 and 39), one can conclude that stateful firewall and/or IPS failure is a direct result of deliberate or inadvertent DDoS attacks.

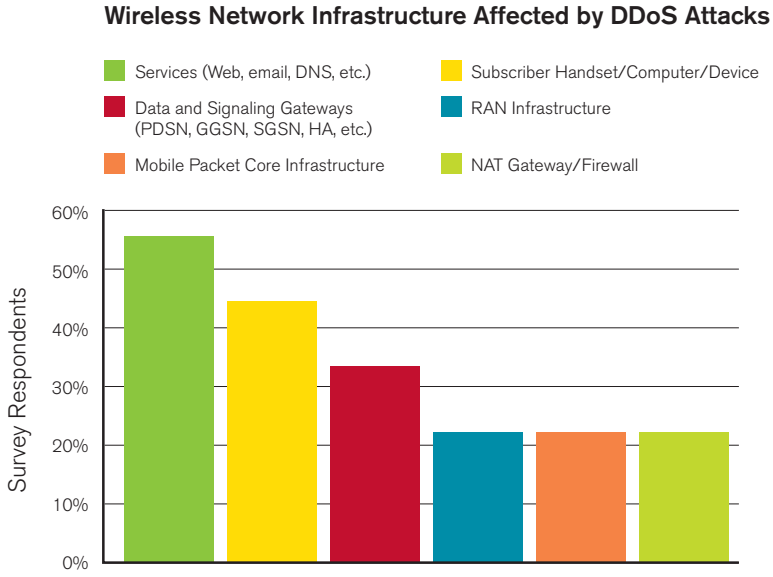

Figure 78
Source: Arbor Networks, Inc.

Figure 79 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, Diameter servers, and even GTP tunnels and SMS gateways.

Layer 7 DDoS Attacks Against Wireless Network Infrastructure

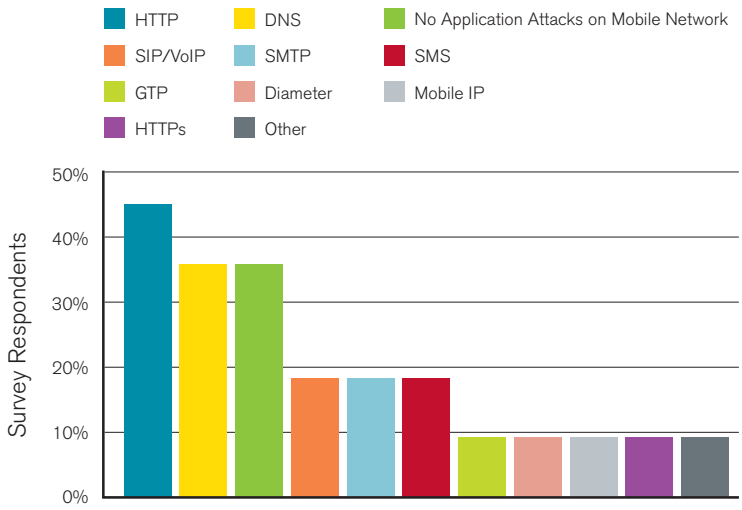

Figure 79
Source: Arbor Networks, Inc.

As illustrated in Figure 80, 50 percent of respondents indicated that they have observed outbound/crossbound DDoS attacks originating from botted or abused subscriber nodes. Given the reported network visibility disadvantages previously described, we believe this statistic may also be understated.

Outbound/Crossbound Attacks from Wireless Subscribers

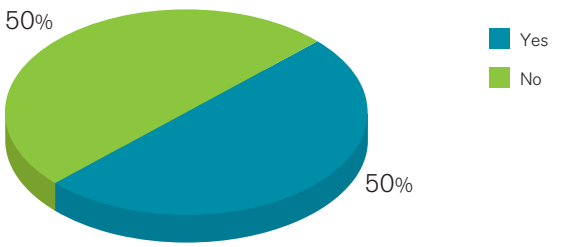

Figure 80
Source: Arbor Networks, Inc.

Figure 81 illustrates that 57 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.

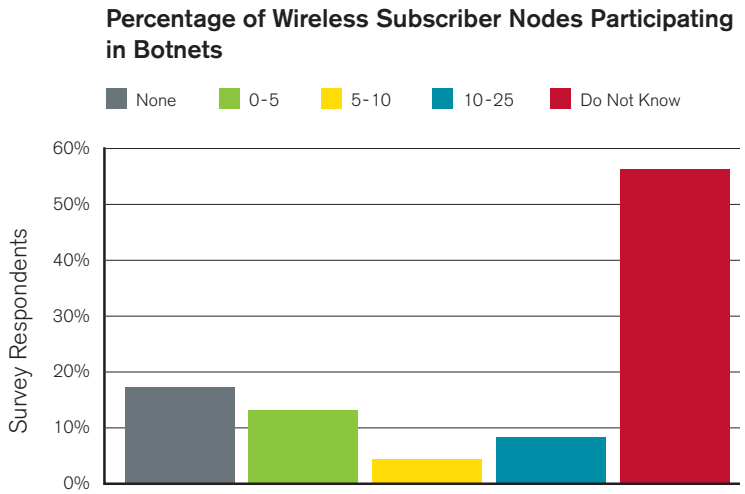

Figure 81
Source: Arbor Networks, Inc.

Wireless operators listed stateful NAT/PAT as a primary security measure to safeguard their packet cores, despite its limitations as a security technology, as previously discussed (Figure 82).

Fifty-seven percent of respondents indicated they have deployed stateful firewalls in their networks as a defensive measure. One-third of respondents have made use of organic security capabilities built into their data and signaling gateways, and 24 percent have deployed IDMS.

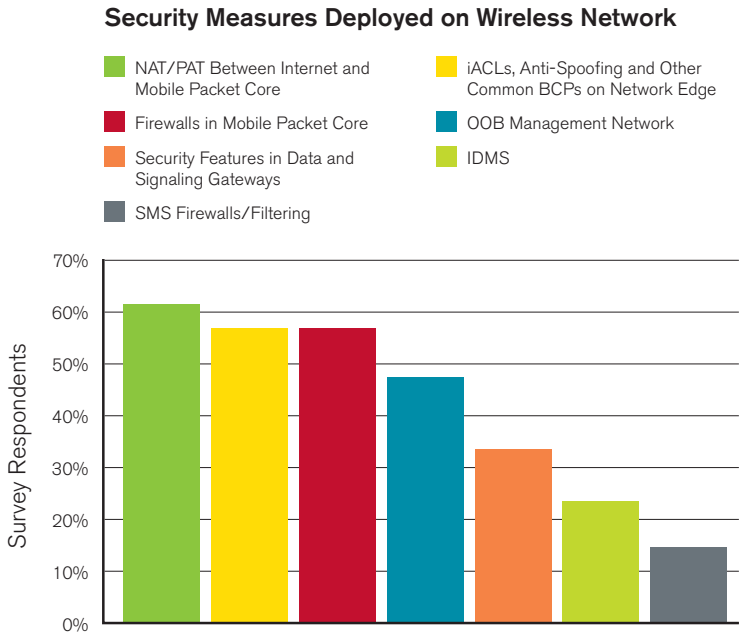

Figure 82
Source: Arbor Networks, Inc.

Figure 83 illustrates that 58 percent of respondents indicated that they intend to deploy IPv6 addressing for wireless subscriber nodes within the next 12 months, while 42 percent have no plans to do so at this time. None of the respondents have deployed IPv6 on their production mobile networks as of this writing.

With a few notable exceptions, the fastest-growing category of ISPs—mobile and fixed wireless operators—may also be the least prepared in terms of network visibility and control, and overall ability to defend themselves and their customers against attack. In many cases, the security postures of mobile and fixed wireless operators approximate those of wireline operators 8 to 10 years ago. As discussed in the section of this report entitled *IDC Operator Observations* (page 39), 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

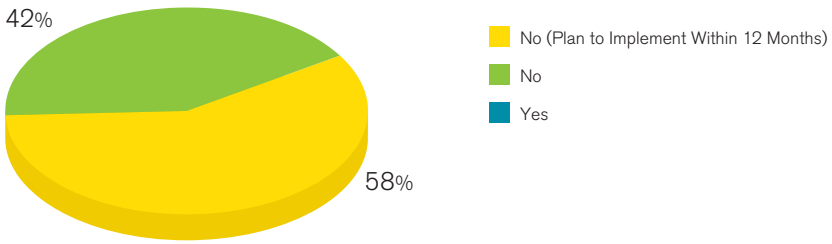

Figure 83
Source: Arbor Networks, Inc.

DNS and DNSSEC Migration Observations

A full 86 percent of respondents operate DNS servers on their networks (Figure 84). Seventy-two percent have either assigned responsibility for their DNS infrastructure to their main operational security group or to a dedicated DNS security team (Figure 85, page 51).

DNS and DNSSEC Migration Observations

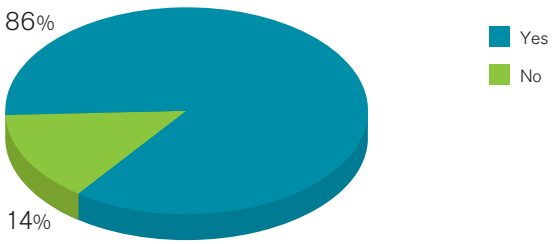

Figure 84
Source: Arbor Networks, Inc.

Twenty-eight 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 (up to 100 Gbps observed to date) DNS reflection/amplification attacks.

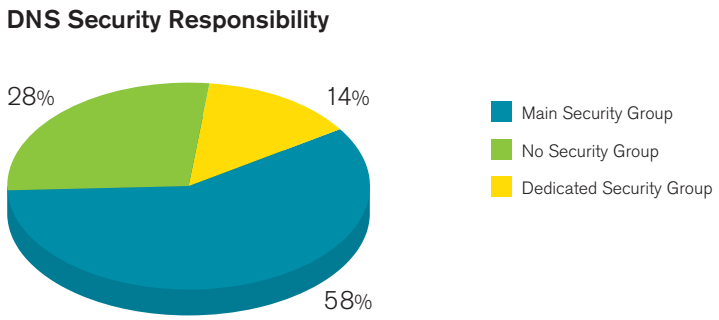

Figure 85
Source: Arbor Networks, Inc.

Seventy-nine percent of respondents have implemented the BCP of restricting recursive lookups by their DNS servers to queriers located either on their own networks or on those of their end customers (Figure 86), while 21 percent have not yet done so.

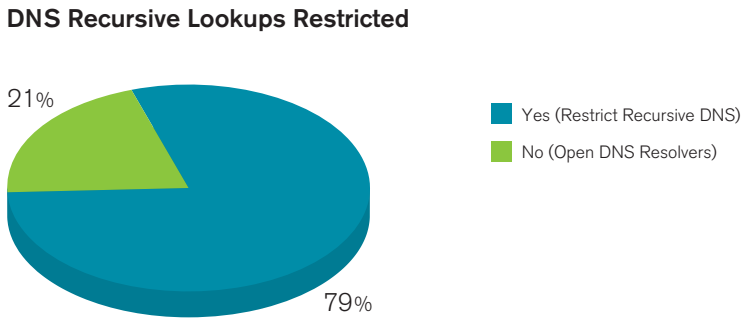

Figure 86
Source: Arbor Networks, Inc.

As indicated in Figure 87, nearly one-third of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period. While DNS is a critical element of the Internet control plane, it often does not receive the architectural, operational, scalability and attack mitigation resources necessary to maintain availability in the face of attack. As a result, DNS has emerged as 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 large number of misconfigured DNS open recursors, coupled with the lack of anti-spoofing deployments, allows attackers to launch overwhelming DNS reflection/amplification attacks.

Customer-Visible DNS Outages Due to DDoS Attacks

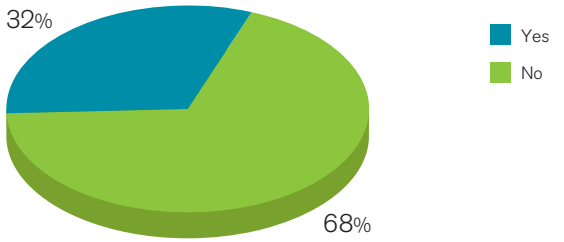

Figure 87
Source: Arbor Networks, Inc.

Only 30 percent of respondents have experienced DNS cache-poisoning attacks directed to or through their DNS infrastructures during the survey period (Figure 88).

DNS Cache-Poisoning Attacks Observed

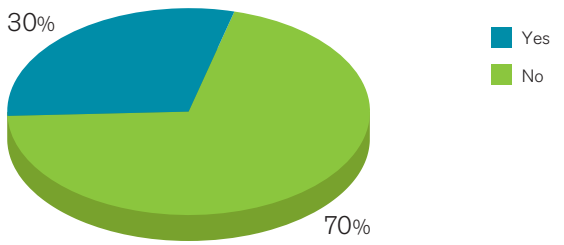

Figure 88
Source: Arbor Networks, Inc.

DNSSEC migration was noted in the 2009 *Worldwide Infrastructure Security Report* as a major challenge facing network operators in 2010; the fact that a solid plurality of 41 percent of survey respondents indicated that they have no definite plans to deploy DNSSEC at this time (Figure 89) confirms this prediction. However, 35 percent of respondents indicated that they do in fact plan to implement DNSSEC within the next 12 months.

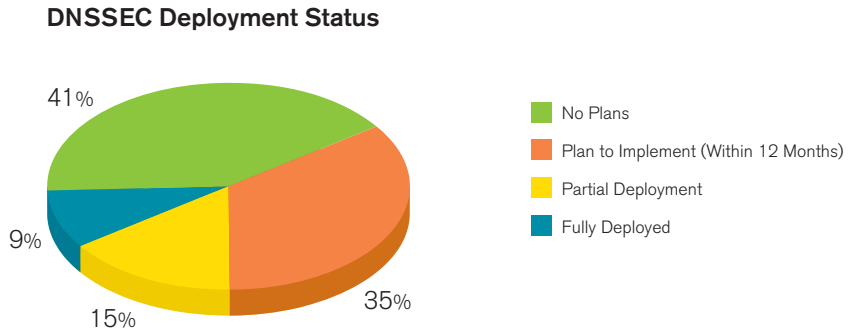

Figure 89
Source: Arbor Networks, Inc.

As illustrated in Figure 90, three-quarters of respondents stated that they do not foresee any problems with DNSSEC deployment due to the lack of EDNS0 and/or TCP/53 DNS support on the Internet at large.

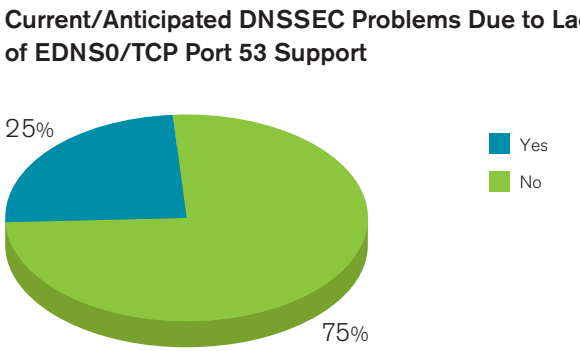

Figure 90
Source: Arbor Networks, Inc.

Sixty-nine 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 91). Interestingly, just after this report's survey was completed and opened for respondents to participate, Arbor observed several instances of DNSSEC-enabled reflection/amplification attacks taking place in several geographies simultaneously.

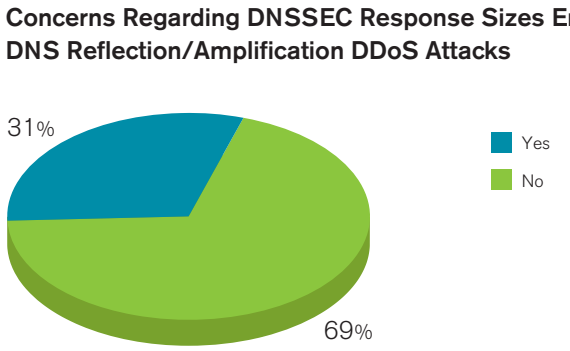

Figure 91
Source: Arbor Networks, Inc.

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

> "Yes, DNSSEC is a more complex and 'interactive' infrastructure to maintain."

> "We have concerns with regards to key rollover, operational issues with name servers that don't currently support or implement DNSSEC, and issues with DNSSEC validation at various levels of the recursive infrastructure."

> "Our main concerns are around customer comprehension and uptake."

> "It seems the only reason the root was signed was the accompanying hoopla generated by Dan Kaminsky's novel cache-poisoning attack. There was a noticeable lack of an actual immediate threat that warranted the sudden change in direction. Time will tell if this was worth it—I'm a bit skeptical that it was."

VoIP Observations

Fifty-five percent of respondents indicated that they offer VoIP services to their end customers (Figure 92). Of that respondent pool, 40 percent indicated that there is no security group within their organizations with formal responsibility for securing the VoIP service delivery infrastructure (Figure 93, page 55).

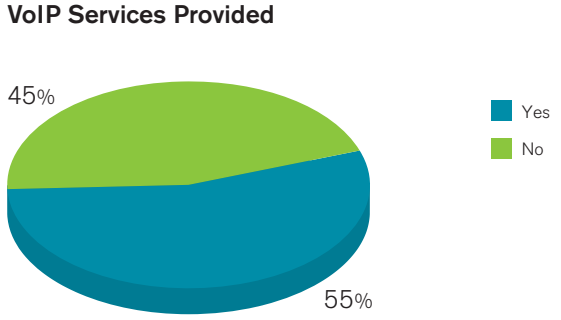

Figure 92
Source: Arbor Networks, Inc.

Responsibility for VoIP Infrastructure/Services Security

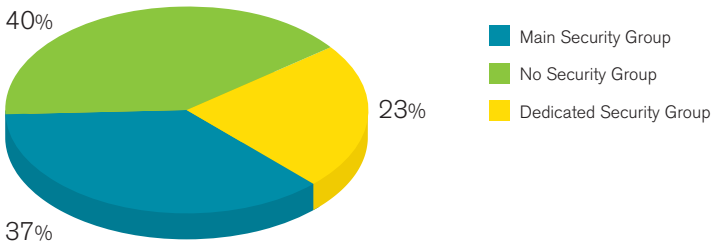

Figure 93
Source: Arbor Networks, Inc.

As noted in Figure 94, while 41 percent of respondents operating VoIP services observed toll fraud taking place in their VoIP infrastructures during the survey period, 59 percent indicated they did not. Of those who observed VoIP toll fraud, 50 percent noted that attackers utilized brute-force attack techniques to commit toll fraud (Figure 95). 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

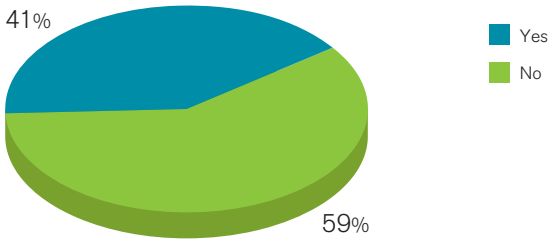

Figure 94
Source: Arbor Networks, Inc.

Brute-Force Attack Techniques Observed in VoIP Toll Fraud

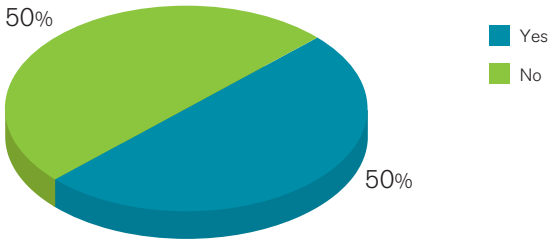

Figure 95
Source: Arbor Networks, Inc.

Sixty-four percent of respondents indicated that caller ID spoofing is a serious concern with regards to their VoIP infrastructure (Figure 96).

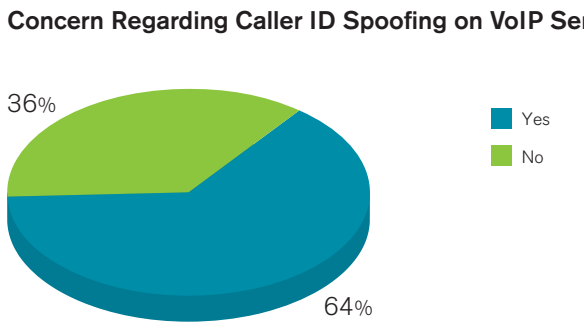

Figure 96
Source: Arbor Networks, Inc.

As illustrated in Figure 97, 45 percent of respondents stated that they use commercial tools to detect attacks against their VoIP infrastructure; 37 percent make use of open-source tools; and 31 percent utilize homegrown detection tools. Meanwhile, 27 percent of respondents indicated that they do not have access to any attack detection tools for use on their VoIP infrastructure.

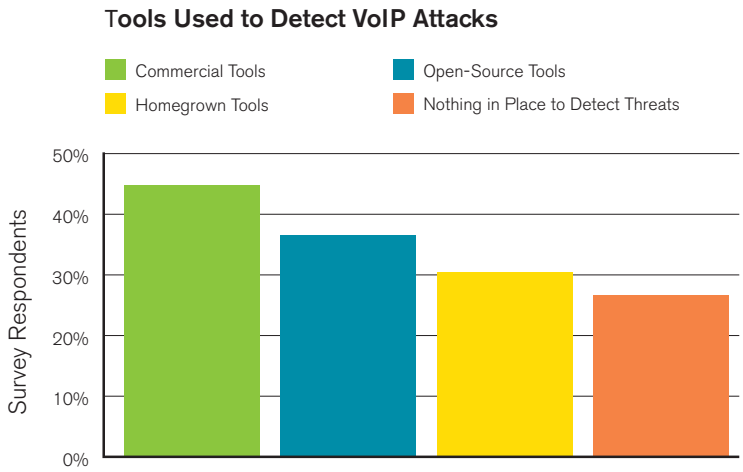

Figure 97
Source: Arbor Networks, Inc.

Figure 98 illustrates that one-quarter of this pool of respondents indicated that they use firewalls as their primary defense mechanism against DDoS attacks. Some 22 percent rely on iACLs, while 16 percent utilize IDMS.

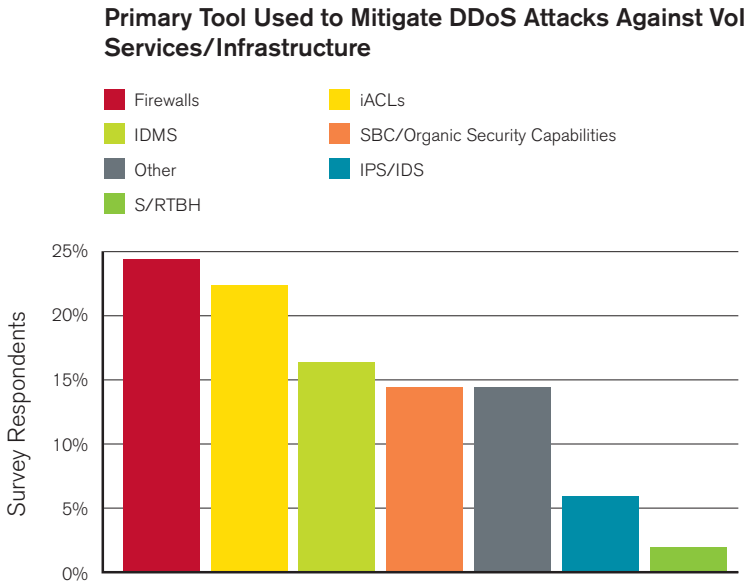

Figure 98
Source: Arbor Networks, Inc.

Sixty-three percent of respondents indicated that they utilize SBCs in their VoIP infrastructure (Figure 99). Fifty-four percent stated that they use additional tools (such as S/RTBH) and IDMS to protect their SBCs against DDoS attack (Figure 100, page 58).

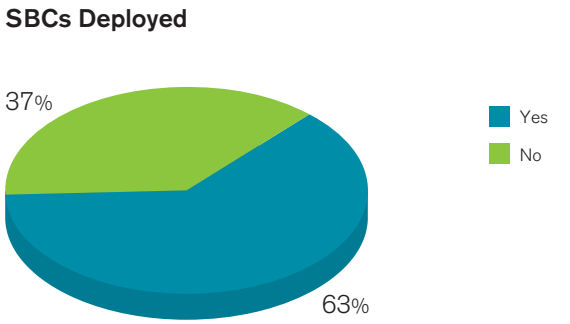

Figure 99
Source: Arbor Networks, Inc.

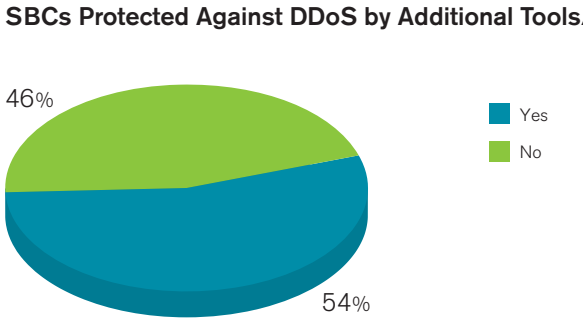

Figure 100
Source: Arbor Networks, Inc.

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 quite positive and constructive, as noted below:

> "This survey has highlighted some areas that my organization may want [to] focus on to improve security."
>
> "A very detailed survey; keep it up and do share the results."
>
> "I read last year's report and found it to be very interesting. I think that IPv6 is a topic that will increase in importance next year."
>
> "Actually, this survey opened my eyes a bit with regards to security-related subjects of which I was not previously aware. Thanks!"

Conclusions

This sixth edition of the Arbor Networks *Worldwide Infrastructure Security Report* comes at a critical juncture for many network operators. As predicted in last year's report, IPv4 address depletion, the transition to IPv6 and DNSSEC are all of great significance to survey respondents.

In this year's report, we observed that attackers have once again upped the ante with regards to DDoS attack volumes, reaching the 100 Gbps mark. This represents a 102 percent increase in observed attack bandwidth year over year and a 1000 percent increase in attack bandwidth since the first report was released in 2005. We also found that while many network operators are investing time and resources to deploy well-known infrastructure BCPs, many are not—or are doing so piecemeal.

We further note that the fastest-growing category of ISPs—mobile and fixed wireless broadband operators—are also the least-prepared organizations in terms of network visibility, network control, and overall ability to successfully defend themselves and their customers against attack. These operators are balancing an overwhelming array of threats with conflicting budget pressures and business objectives.

IDC operators are increasingly at the forefront of defending against DDoS attacks. Many respondents in this category have been saddled with the legacy of industry misunderstanding regarding the inadvisability of placing stateful firewalls and IPS devices in front of servers—where there is in fact no state to inspect. As a result, they are increasingly experiencing customer-impacting outages due to DDoS attacks.

With regards to IPv6 migration, many network operators are both resigned to and frustrated by the long series of hurdles they must overcome to achieve IPv6 parity with their current IPv4 networks.

DNS continues to represent both a highly vulnerable target for DDoS attacks and a preferred attack vector due to the relative lack of resources and attention paid by network operators to DNS service resiliency, scalability and best current practices. Many operators hold the opinion that investing time and resources in DNSSEC migration appears to offer little in the way of immediate dividends. However, the increased size of DNSSEC responses has resulted in an increase in DNS reflection/amplification attacks observed in the wild.

Survey respondents continue to view law enforcement activities in the arena of Internet crime as largely ineffective. However, operators are eager for government engagement and involvement in operational security matters via CERTs and CSIRTs. Vetted operational security groups are also seen as being highly effective in marshaling resources to defend against attacks in real time. A majority of this year's respondents are active participants in such organizations.

The 2010 *Worldwide Infrastructure Security Report* reflects both a continuation and expansion of the same basic concerns expressed by operators in the 2009 report, with additional details regarding the challenges faced by specific categories of network operators clearly articulated.

Finally, it is our view that there is at least one positive side-effect of recent high-profile, ideologically motivated DDoS attacks, such as those associated with the WikiLeaks[3] affair, namely that awareness about the importance of maintaining availability for all Internet-connected organizations has been elevated to the executive level. Overall, we believe this executive visibility is a net positive that will hopefully serve as a motivating factor to correct some of the resourcing and implementation deficits described in this report.

3 http://asert.arbornetworks.com/2010/11/wikileaks-cablegate-attack

About the Authors

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

Roland Dobbins has 25 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 Operations, 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, Consulting Engineer, 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. Craig Labovitz, Chief Scientist, Arbor Networks
clabovitz@arbornetworks.com

Craig Labovitz brings extensive experience in network engineering and research to Arbor. Previously, he served as a network researcher and scientist for Microsoft Corporation. He also spent nine years with Merit Network, Inc. and the University of Michigan as a senior backbone engineer and director of the Research and Emerging Technologies group.

Dr. Labovitz's work at Merit included design and engineering on the NSFNet backbone and Routing Arbiter projects. He also served as the director of several multimillion dollar grants from the National Science Foundation for network architecture and routing protocol research. Dr. Labovitz received his PhD and MSE from the University of Michigan.

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, Systems 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
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
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
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 GPRS 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

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

P

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

Q

QoS quality of service

R

RAN radio access network
RDP Remote Desktop Protocol
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

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

WISR/EN/0111

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for converged carrier networks and next-generation data centers, including more than 70 percent of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the Active Threat Level Analysis System (ATLAS®). Representing a unique collaborative effort with 100+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.