ARBOR®
NETWORKS

2012 Infrastructure Security Report

8th Annual Edition

Key Findings in the Survey*

- **Advanced Persistent Threats (APT) a top concern for service providers and enterprises**
  - This year's survey found an increased level of concern over 'botted' or compromised machines on service provider networks
  - Looking ahead, there is even more concern about APT, industrial espionage, data exfiltration and malicious insiders
- **DDoS: Attack Sizes Plateau in Trend Towards Complex Multi-Vector Attacks**
  - HTTP and DNS most common application layer targets
  - Growth in proportion of respondents seeing attacks targeting HTTPS
  - Largest volumetric attacks in 60 – 100 Gbps range
- **Data Centers Increasingly Becoming Victimized**
  - 94% of datacenters seeing DDoS attacks regularly
  - Just over a third see firewalls fail due to DDoS attacks
  - As more companies move their services to the "cloud," shared risk is more of an issue
- **Ideology Is Primary DDoS Driver**
  - Top 3 attack motivations are based on politics, gamesmanship, beliefs and revenge

*Survey time period: Oct 2011 – Sept 2012

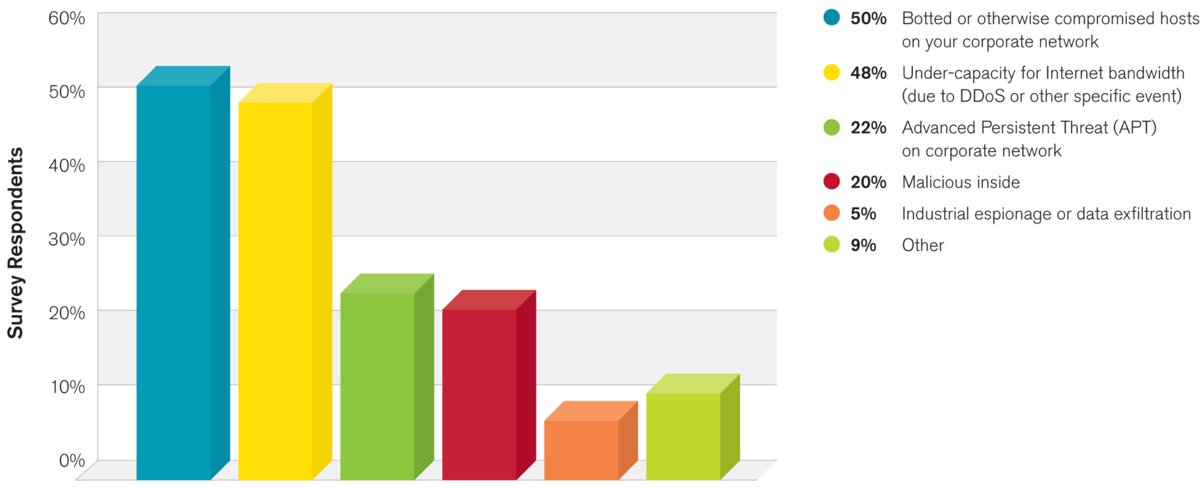
Additional Key Findings

- **Mobile Providers Continue to be Reactive**
  - A full 60 percent of respondents do not have visibility into the traffic on their mobile/evolved packet cores.
  - The economics of consumer subscriber networks do not incent providers to implement security until a problem occurs.
- **DNS Infrastructure Remains Vulnerable**
  - The Internet's name resolution service continue to be both victimized by DDoS and used as an attack tool
- **IPv6 Deployments Quickly Becoming Pervasive**
  - 80% of respondents either have IPv6 implemented or will do within the next 12 months
  - More focus on availability of IPv6 services
- **Operational Security Resources still Challenged, Limited Law Enforcement Involvement**
  - Just under a quarter of respondents have NO dedicated security resources
  - A half of respondents NEVER practice their incident handling processes
  - More than half of respondents do NOT refer security incidents to law enforcement.

ARBOR® NETWORKS

Internal Network Threats: APT a Growing Concern

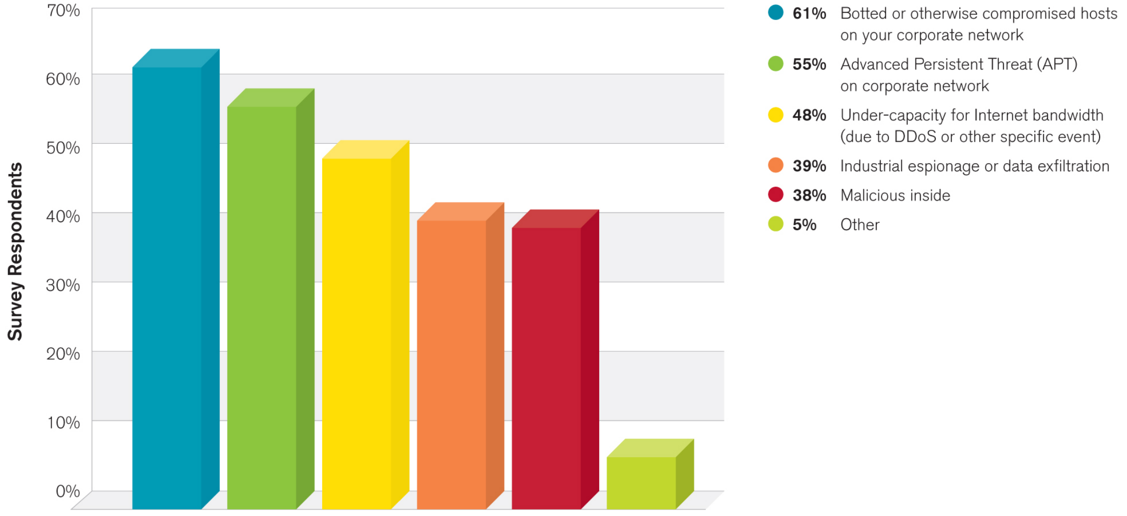
Internal Network Security Threats



Source: Arbor Networks, Inc.

- Botted or compromised hosts have been experienced by half of respondents on their internal networks

Internal Network Security Concerns



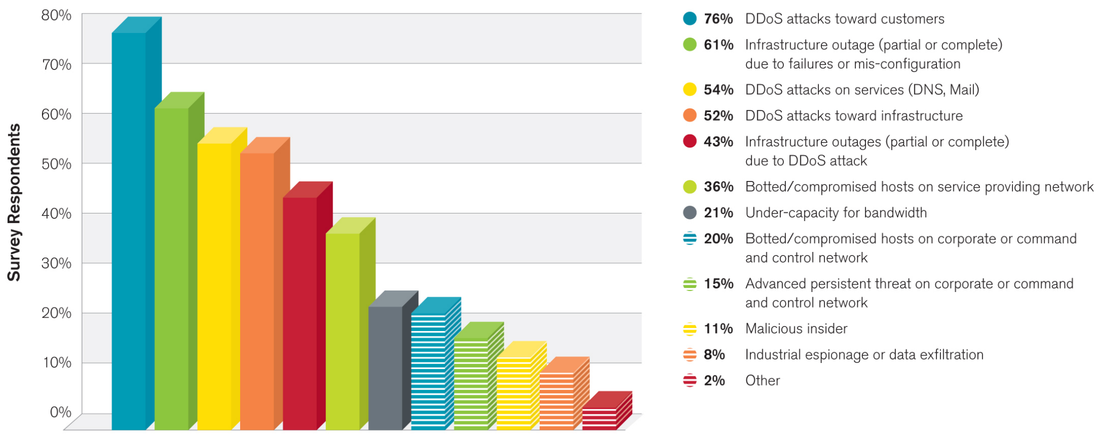
Source: Arbor Networks, Inc.

- Clear rise in concerns over APT and Industrial espionage for next twelve months, despite lack of experience so far

The DDoS Threat Tops Mindshare

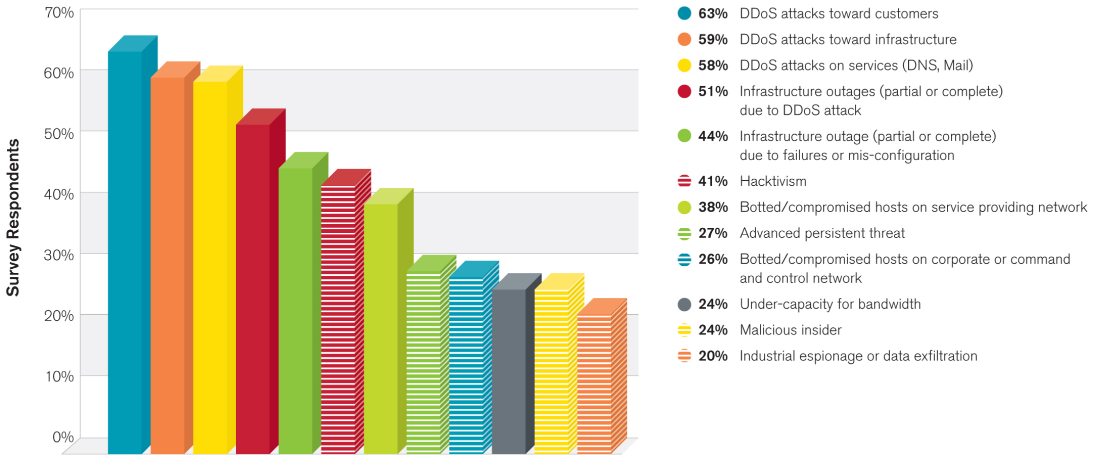
- 4 of the top 5 threats seen over the last 12 months are DDoS related
- The top 4 perceived threats for the next 12 months are DDoS related
- Misconfiguration in 5th place, despite consistently high showing in observed threats

Most Significant Operational Threats



Source: Arbor Networks, Inc.

Operational Security Concerns in the Next 12 Months

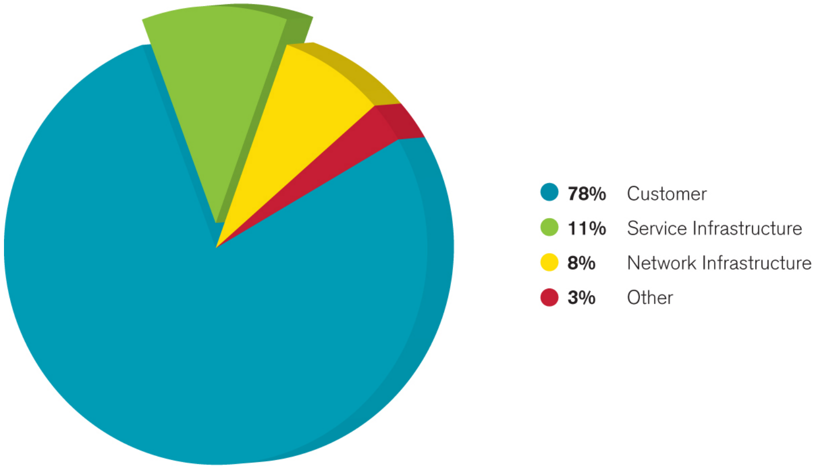


Source: Arbor Networks, Inc.

ARBOR®
NETWORKS

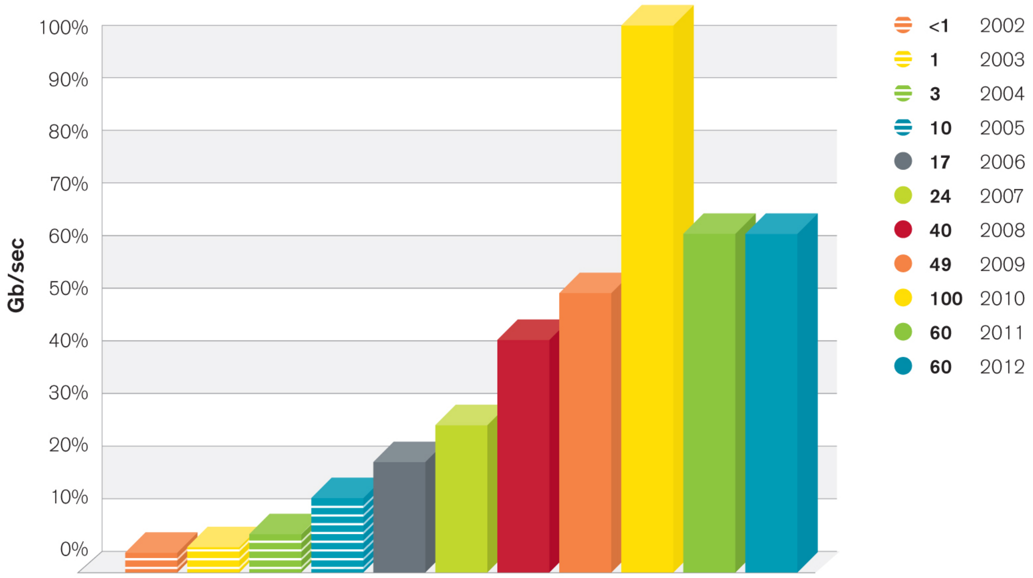
Large DDoS Attacks Still Occurring

Target of Largest DDoS Attacks



Source: Arbor Networks, Inc.

Size of Largest Reported DDoS Attack (Gbps)



Source: Arbor Networks, Inc.

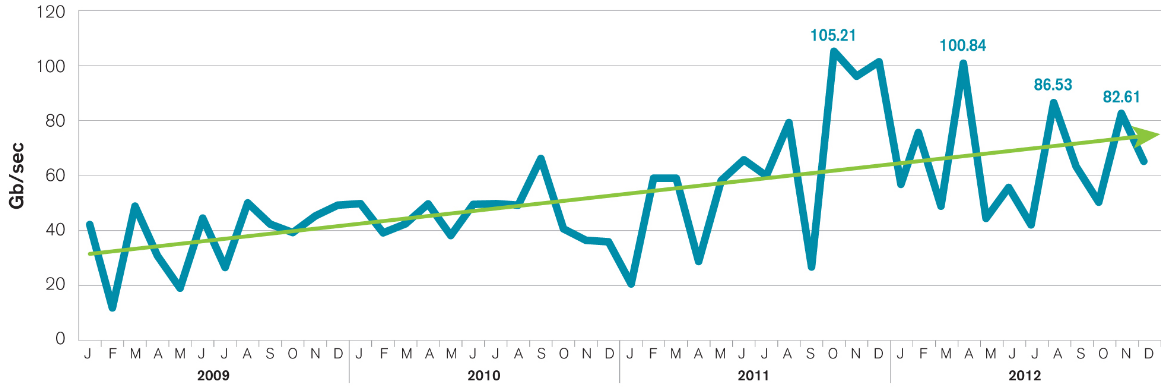
- Service provider customers are most common targets of the largest reported attacks
- Largest reported attack at same level as last year, 60Gbps
  - ATLAS continues to report attacks in the 80 – 100Gbps range
  - Attacks seem to have plateaued at around 100Gbps top-end for past 3 years

ATLAS Attack Sizes

- Peak attacks at 80 - 100Gbps in 2012

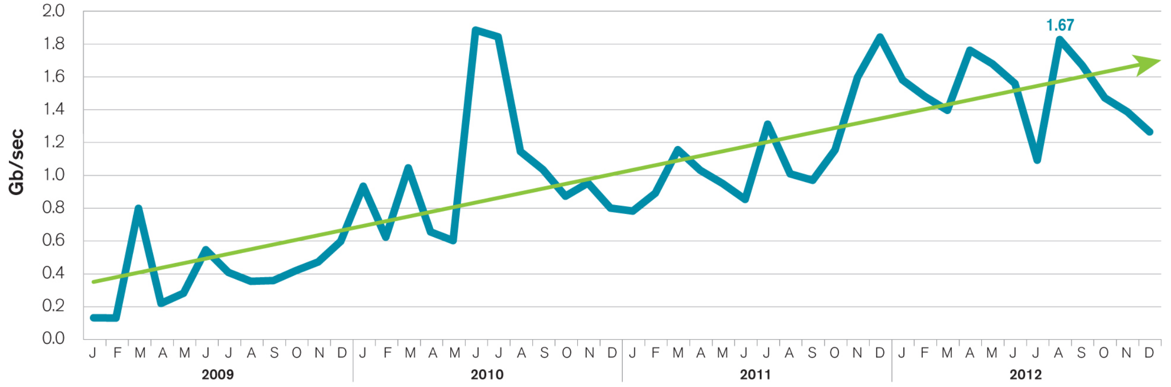
- Average attacks now consistently over 1Gb/sec

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



Source: Arbor Networks, Inc.

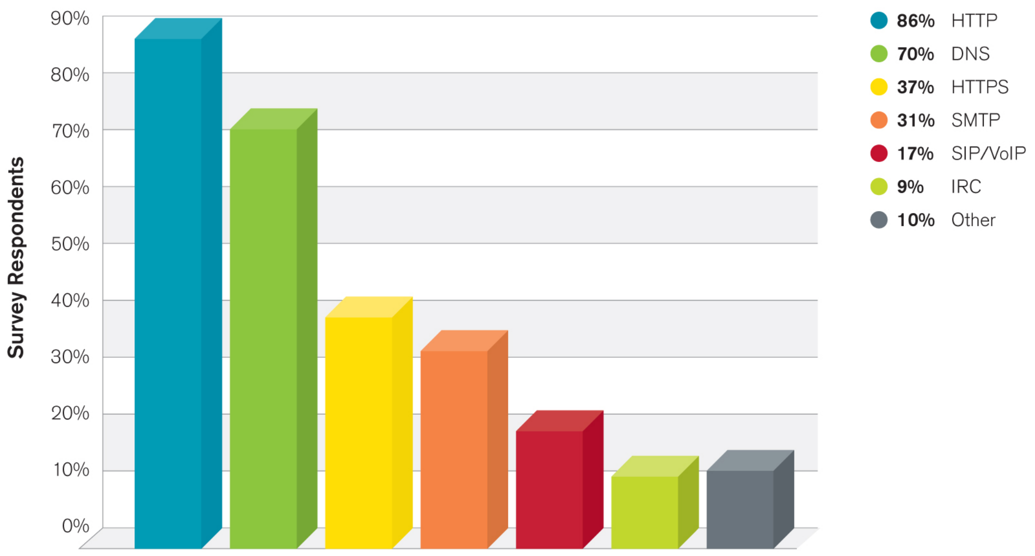
ATLAS Average Monitored Attack Sizes Month-By-Month (January 2009-Present)



Source: Arbor Networks, Inc.

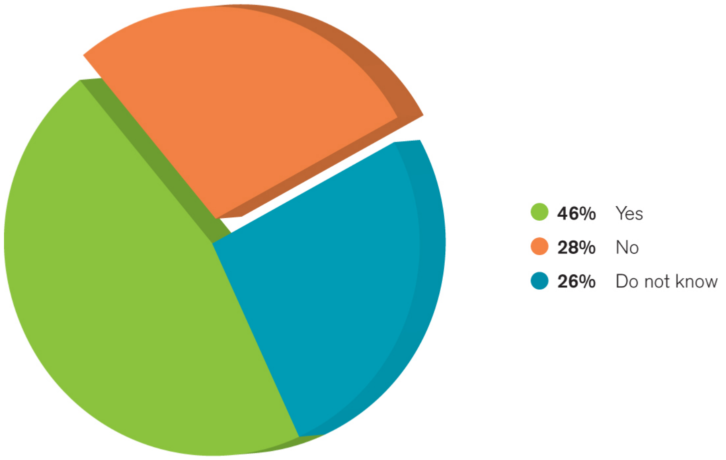
Application Layer / Multi-Vector Attacks Are Rising

Targets of Application-Layer Attacks



Source: Arbor Networks, Inc.

Multi-Vector DDoS Attacks



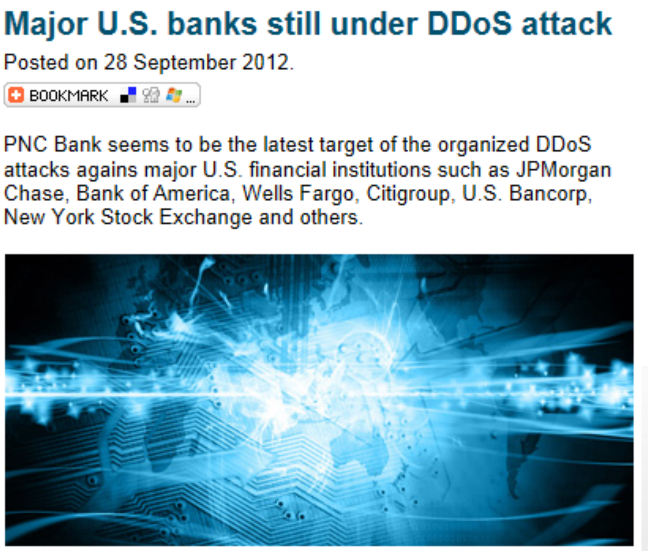
Source: Arbor Networks, Inc.

- HTTP and DNS services most frequently targeted by application layer attacks.
- In a 60% increase over last year, nearly half of respondents now seeing multi-vector attacks
  - Multi-vector attacks are a concern as they generally require layered defenses for successful mitigation
  - Q4 2012 Financial Attacks were a good example

ARBOR® NETWORKS

Recent Financial Attacks aka "Operation Ababil:" Multi-Vector DDoS On A New Level

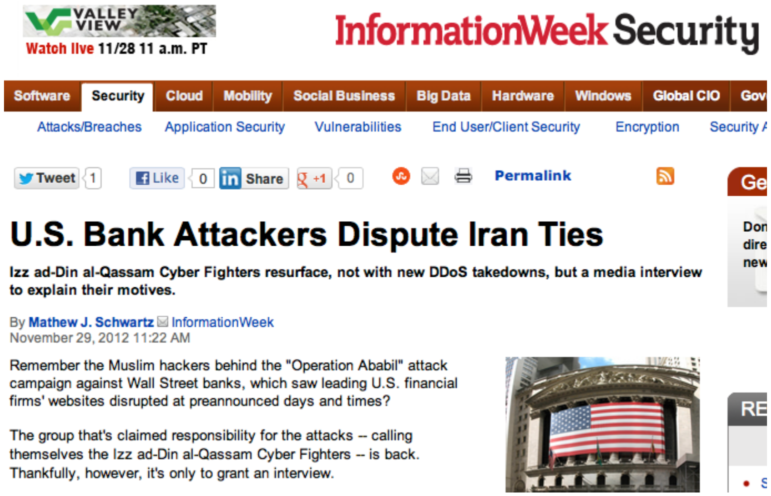
- Compromised PHP, WordPress, & Joomla servers
- Multiple concurrent attack vectors
  - GET and POST app layer attacks on HTTP and HTTPS
  - DNS query app layer attack
  - Floods on UDP, TCP Syn floods, ICMP and other IP protocols
- Unique characteristics of the attacks
  - Very high packet per second rates per individual source
  - Large bandwidth attack on multiple companies simultaneously
  - Very focused



Major U.S. banks still under DDoS attack

Posted on 28 September 2012.

PNC Bank seems to be the latest target of the organized DDoS attacks agains major U.S. financial institutions such as JPMorgan Chase, Bank of America, Wells Fargo, Citigroup, U.S. Bancorp, New York Stock Exchange and others.



U.S. Bank Attackers Dispute Iran Ties

Izz ad-Din al-Qassam Cyber Fighters resurface, not with new DDoS takedowns, but a media interview to explain their motives.

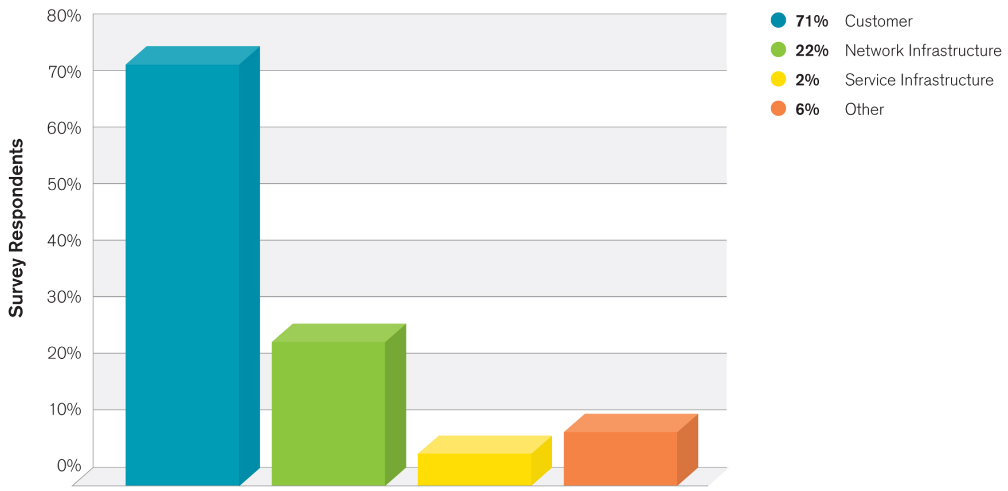
By Mathew J. Schwartz InformationWeek
November 29, 2012 11:22 AM

Remember the Muslim hackers behind the "Operation Ababil" attack campaign against Wall Street banks, which saw leading U.S. financial firms' websites disrupted at preannounced days and times?

The group that's claimed responsibility for the attacks -- calling themselves the Izz ad-Din al-Qassam Cyber Fighters -- is back. Thankfully, however, it's only to grant an interview.

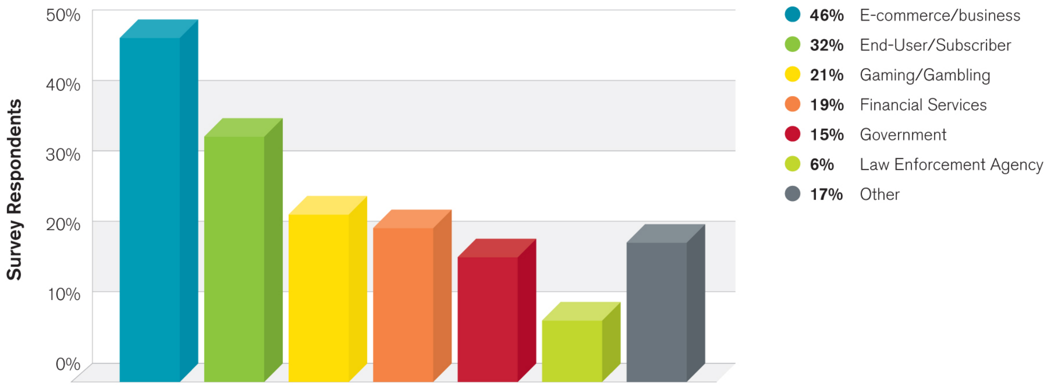
Overall Attack Targets

Monitored Attack Targets



Source: Arbor Networks, Inc.

Targeted Customer Types

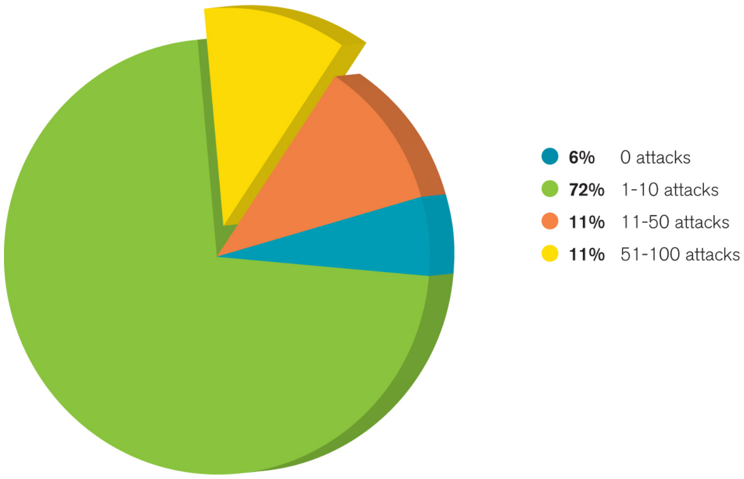


Source: Arbor Networks, Inc.

- Respondent customers are by far the most common target of attacks
- e-commerce / business customers are the most likely targets, followed by end-users / subscribers.
- Financial services and government are a distant fourth and sixth, counter to media coverage and expectation

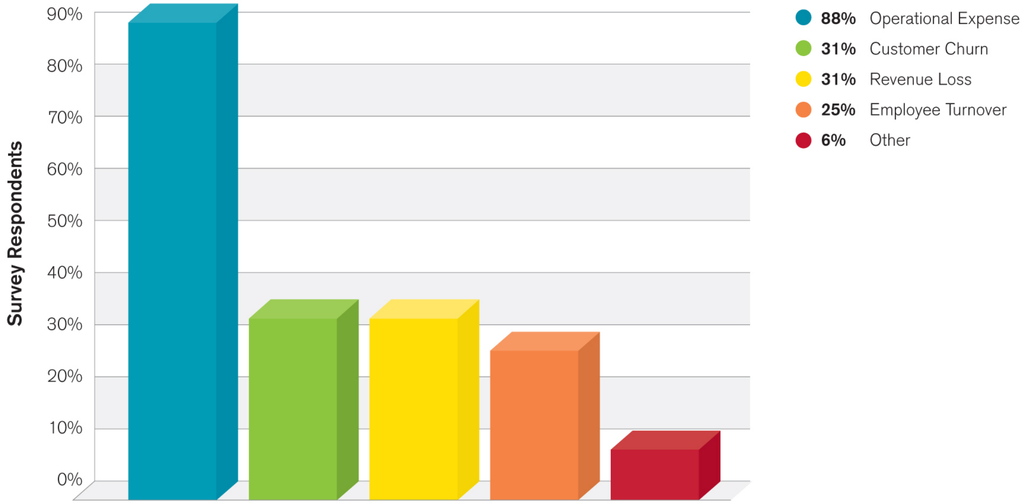
Data Center DDoS Attack and Impact

Frequency of Attacks (Per Month)



Source: Arbor Networks, Inc.

Business Impact of Attacks

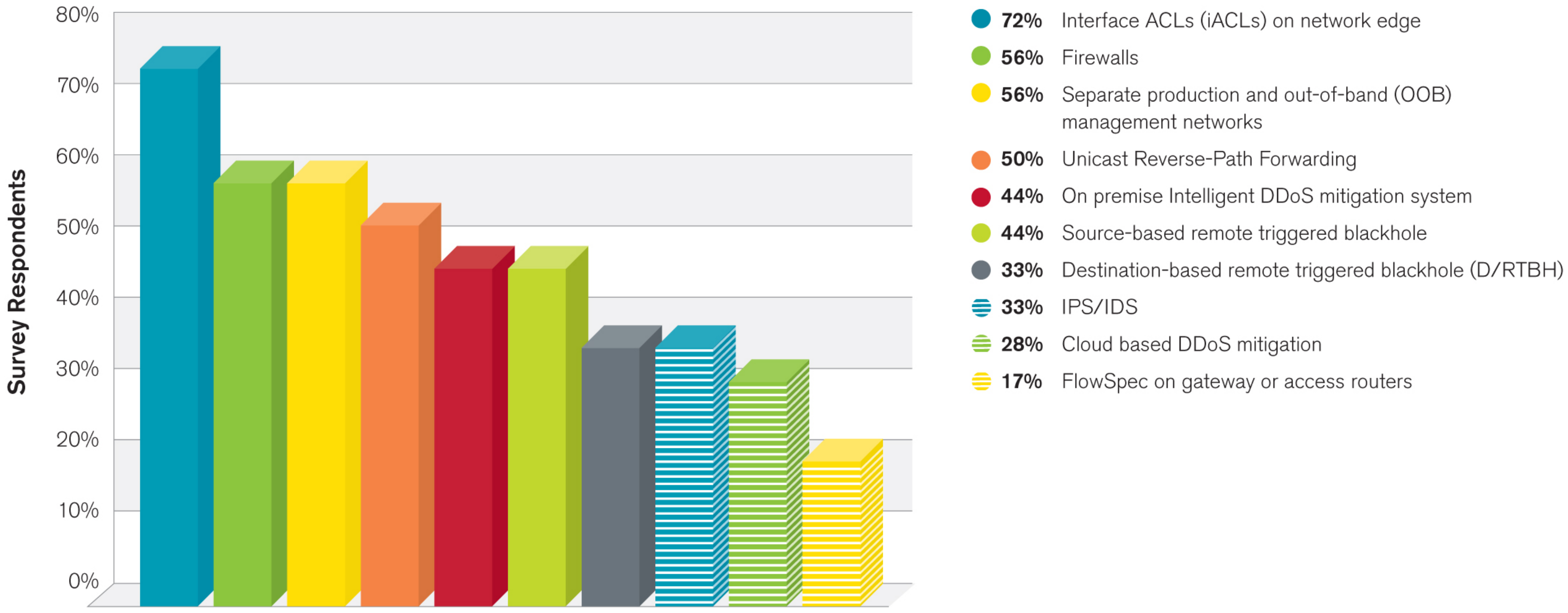


Source: Arbor Networks, Inc.

- 83.3% of respondents now see between 1 and 50 attacks per month.
- Proportion of respondents seeing 0 attacks per month drops from 30% to 5.6%
- Big rise in proportion of respondents seeing attacks targeting infrastructure and infrastructure services.
- Operational costs are main expense for data center operators in dealing with attacks.
  - However nearly a third experience customer churn or revenue loss due to attacks.

Data Center DDoS Mitigation

DDoS Protection Techniques in the Data Center

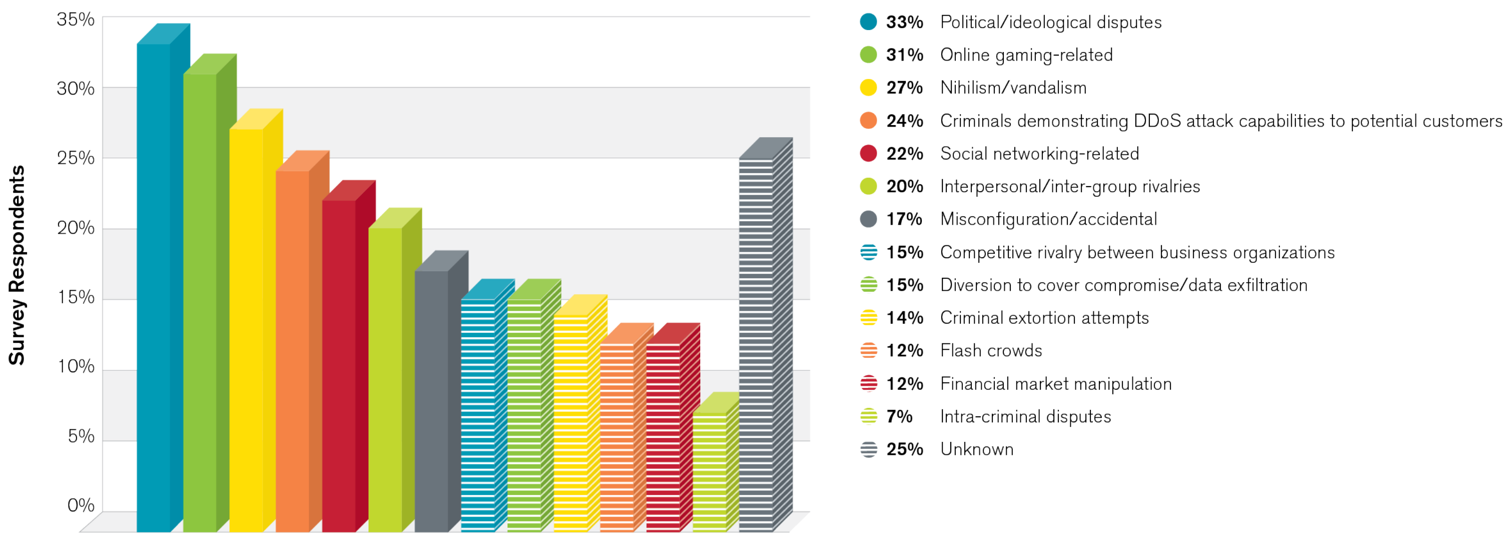


Source: Arbor Networks, Inc.

- 10% increase in use of IDMS and 22% decrease in use of D-RTBH
  - May indicate increased focus on maintaining service availability.
- Big increase in use of firewalls for mitigation
  - 35% saw firewalls fail due to DDoS attacks during the survey period

Top DDoS Motivations

Most Common Motivations Behind DDoS Attacks

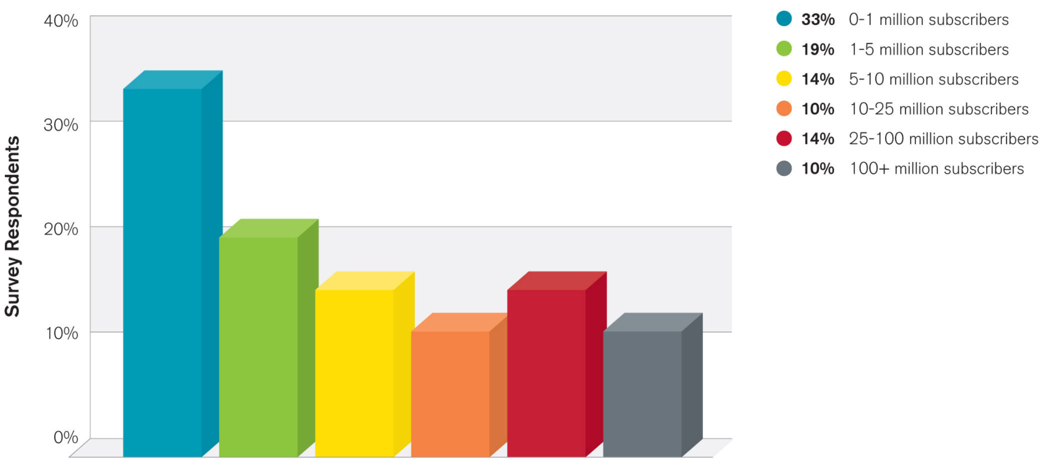


Source: Arbor Networks, Inc.

- Number one motivation is still ideological hacktivism
  - Not surprising given media coverage this year
- On-line gaming up from third to second
- Nearly 15% seeing attacks motivated by extortion, competitive rivalry or as a cover for data exfiltration. DDoS is now a part of more complex cyber attack campaigns.
- Broader range of motivations = higher risk of attack

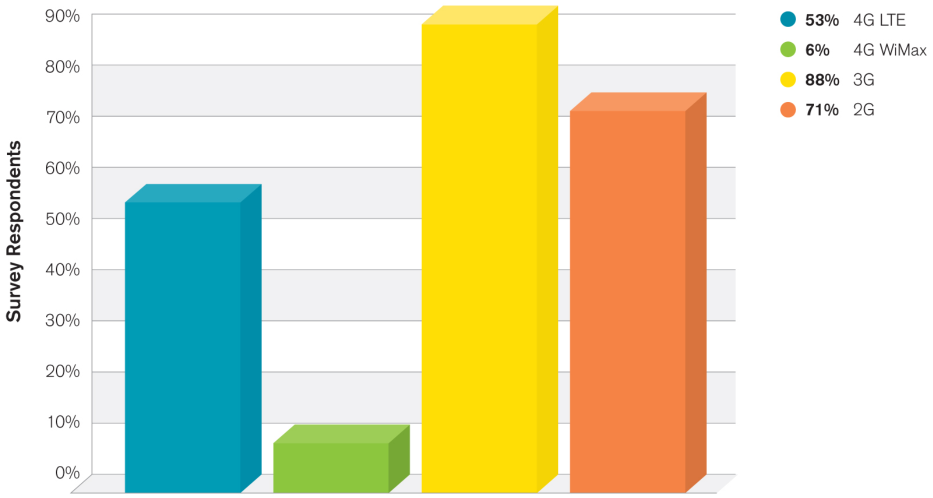
Mobile Respondents and Technologies

Subscriber Base on Wireless Networks



Source: Arbor Networks, Inc.

Deployed Wireless Technologies

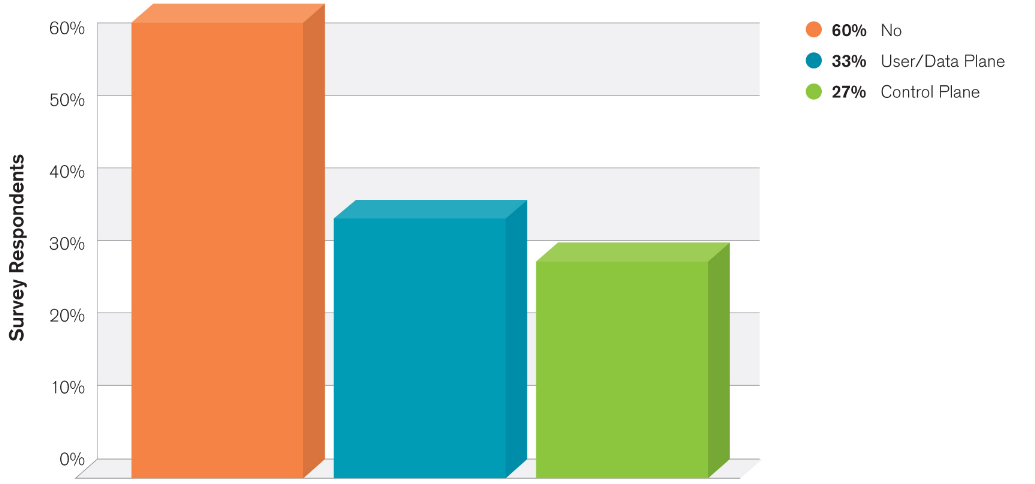


Source: Arbor Networks, Inc.

- 57% offer services to more than 1M subscribers
  - 34% have more than 10M subscribers
- 3G and 2G still dominate
- LTE deployment growing fast, from 28.6% last year to 52.9% this year
  - 33% offering commercial 4G services now, up from 19% last year
  - 44.5% plan for 4G services in 2013/14

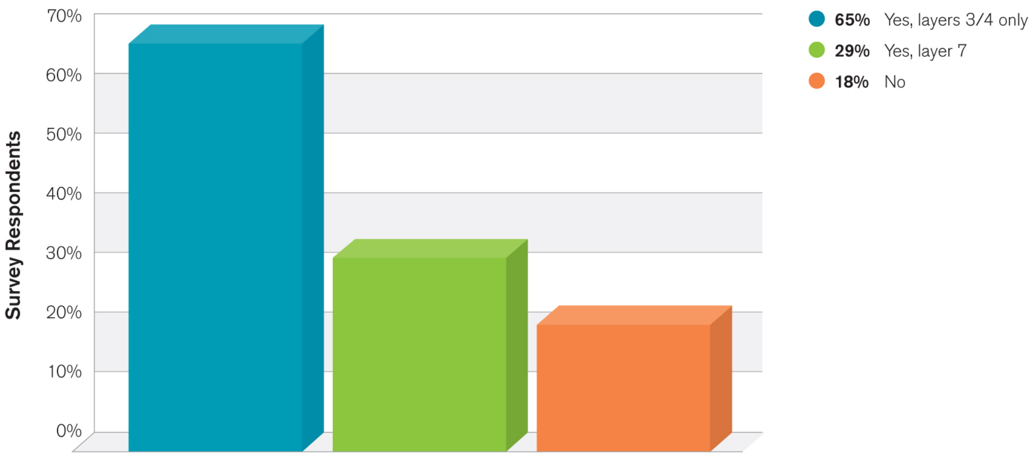
Mobile Traffic Visibility Still an Issue

Visibility of Traffic on Mobile/Evolved Packet Core



Source: Arbor Networks, Inc.

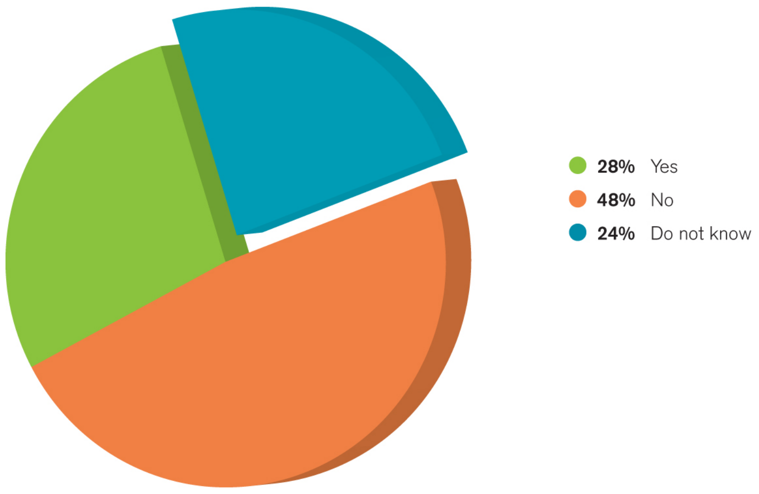
Visibility on Mobile Internet (Gi) Backbone



Source: Arbor Networks, Inc.

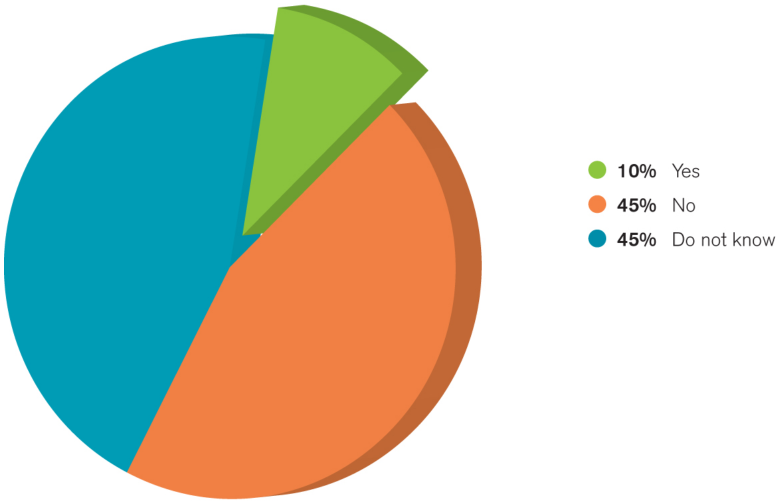
- 33% of respondents saw a customer visible outage due to a security incident, up from 12.5%.
- But, visibility of what is going on is still a key issue:
  - 60% do not have visibility of traffic on their CPC / EPC
  - 18% do not have visibility of traffic at their Gi

Mobile Threat Detection Limitations



Inbound DDoS Attacks Targeted Towards Wireless Network

Source: Arbor Networks, Inc.

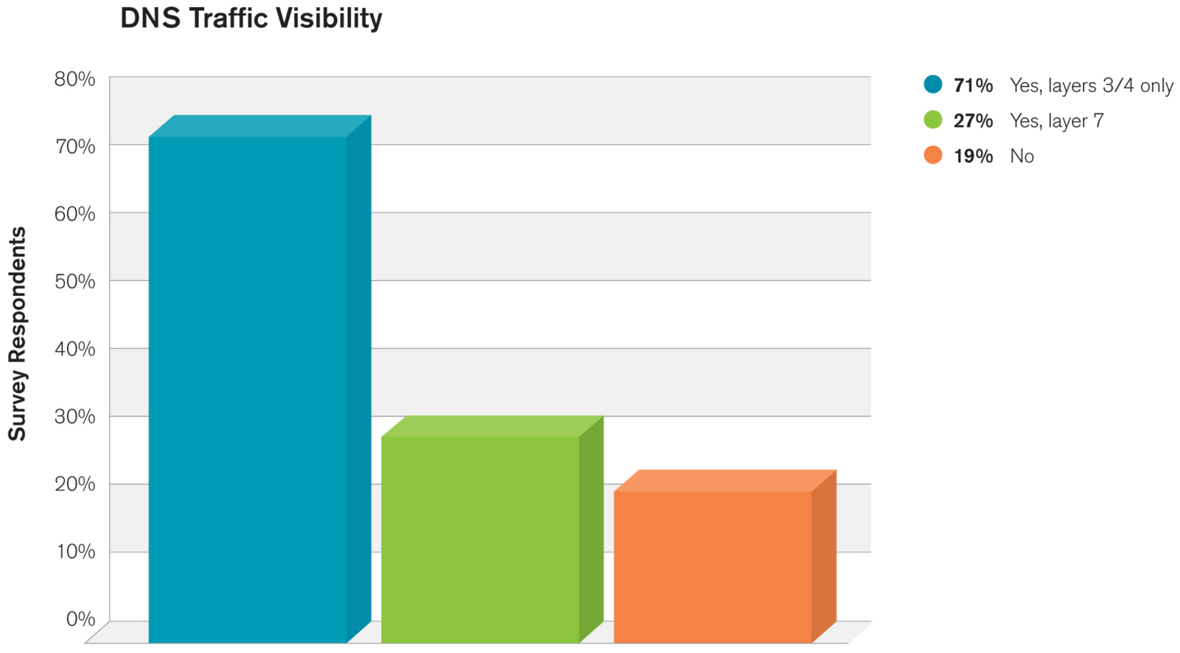


DDoS Attack Impact on Internet (Gi) Infrastructure

Source: Arbor Networks, Inc.

- 28.6% see attacks targeting mobile users, RAN, back-haul or packet core
  - Firewalls and end-users are most commonly affected
- Only 10% of respondents see DDoS attacks impacting their Gi side infrastructure
  - Only targets were DNS servers and routers / links (congestion)
  - Very low given anecdotal conversations
  - 45% don’t know if they are being attacked
- 57% of respondents do NOT know how many compromised subscribers there are on their networks.

DNS Visibility



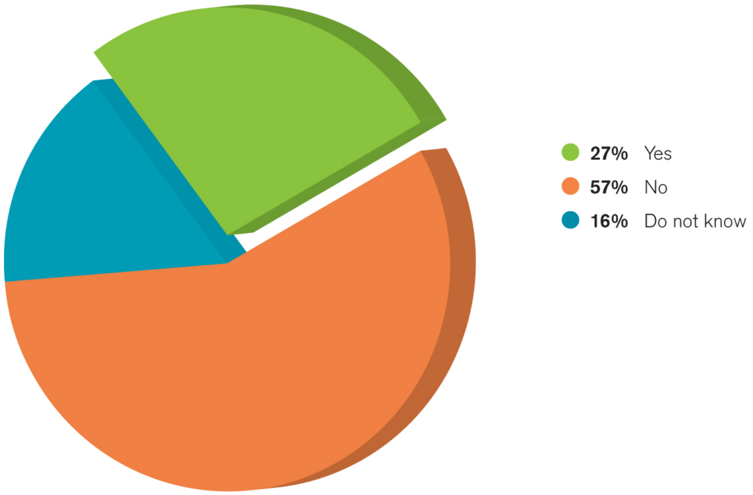
Source: Arbor Networks, Inc.

- 81% of respondents operate DNS infrastructure.
- 19% have NO security team responsible for it
  - An improvement from 23% last year
  - Still not good given the criticality of this service
- Nearly three quarters have good visibility at layers 3/4 , but only just over a quarter have layer 7 visibility
  - Needed to detect some types of attacks etc.

ARBOR® NETWORKS

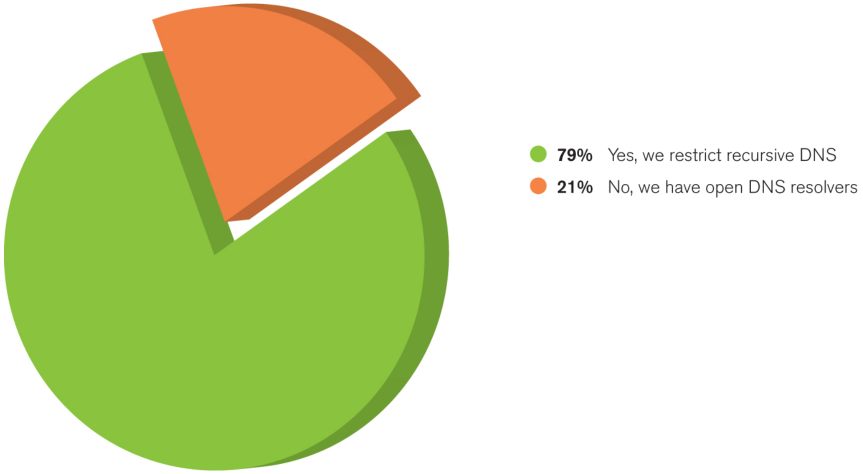
DNS Security

Customer-Impacting DNS Attacks



Source: Arbor Networks, Inc.

DNS Recursive Lookups Restricted

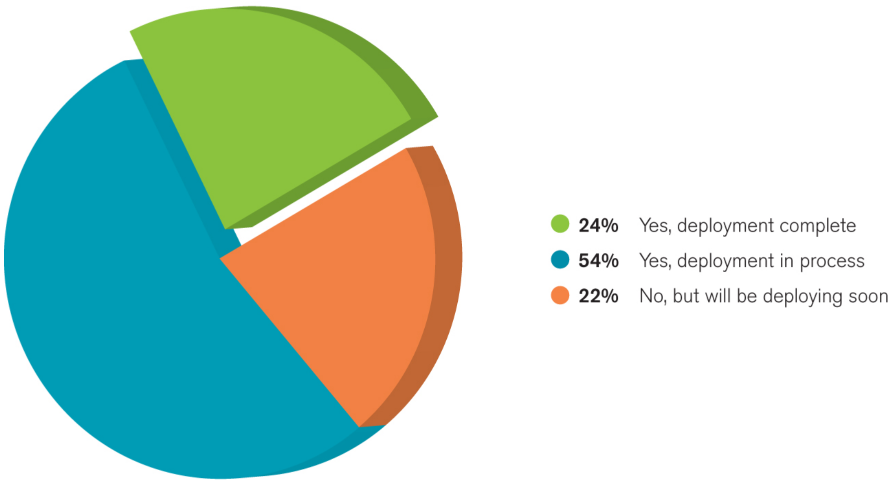


Source: Arbor Networks, Inc.

- Just over a quarter have seen customer impacting DDoS attacks against DNS infrastructure
  - 40.8% have seen attacks against authoritative servers
  - 24% have seen attacks against recursors
- 21% of respondents do NOT restrict recursive look-ups
  - Same result as last year
  - Contributes toward reflective amplification attacks
- The majority of respondents have NOT seen issues with DNSSEC

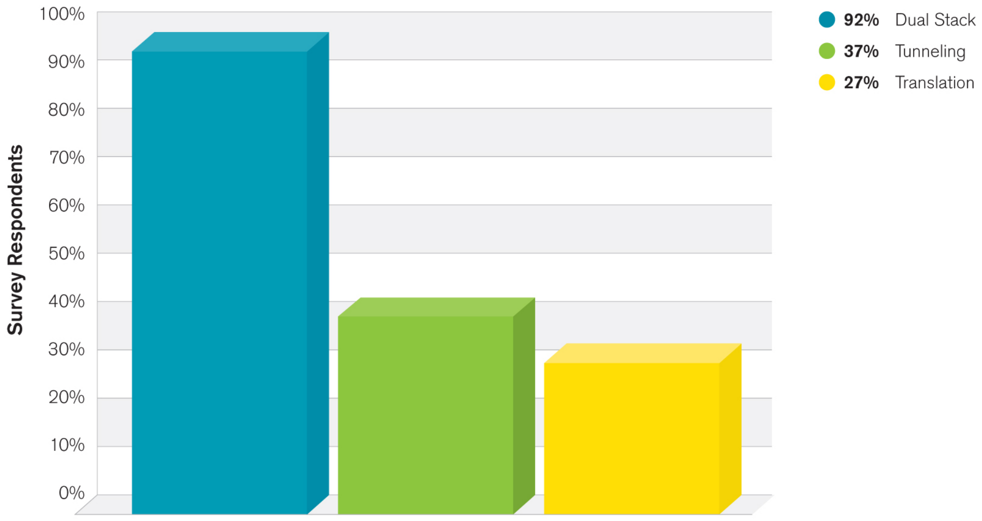
IPv6 Roll-Out Moves Forward

IPv6 Deployment Progress



Source: Arbor Networks, Inc.

IPv6 Migration Strategy



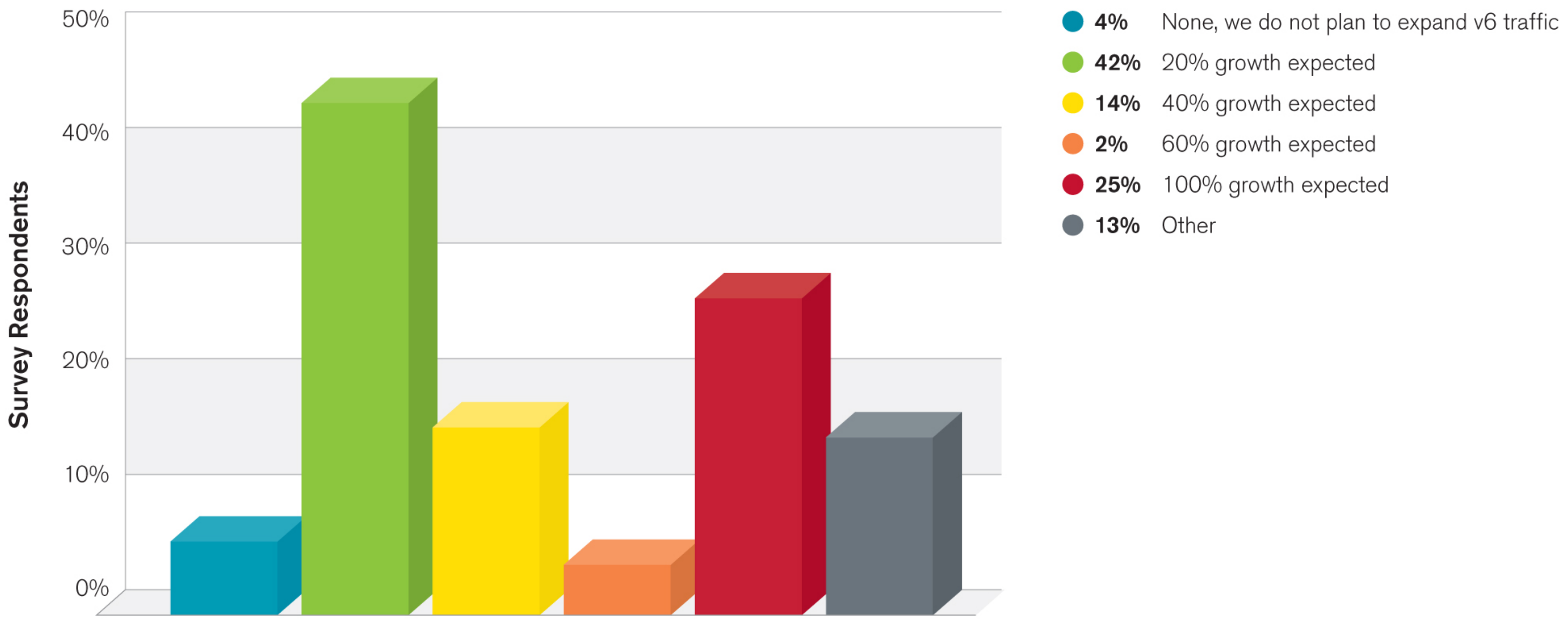
Source: Arbor Networks, Inc.

- 80% of respondents either have IPv6 implemented or will do within the next 12 months
  - 24.1% have already <u>completed</u> their roll-out
- IPv4 address space exhaustion is NOT seen as a concern by the majority of respondents
- Dual-stack seems to be the most widely implemented migration strategy

ARBOR® NETWORKS

IPv6 Growth

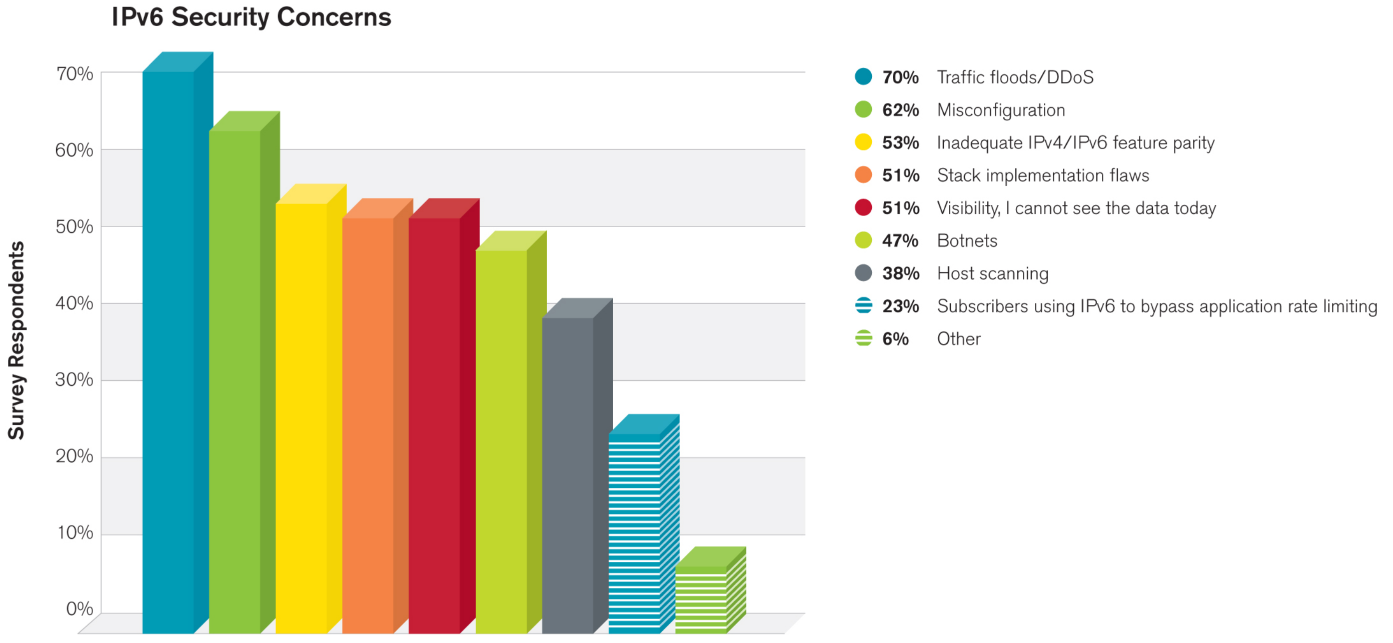
IPv6 Traffic Growth



Source: Arbor Networks, Inc.

- Nearly half of respondents only anticipate 20% growth in IPv6 traffic volume over next twelve months
- One quarter expect more than 100%
- ATLAS data shows that IPv6 is growing at more than 100% per year, but is still only a small fraction of IPv4 traffic

IPv6 Threats and Concerns

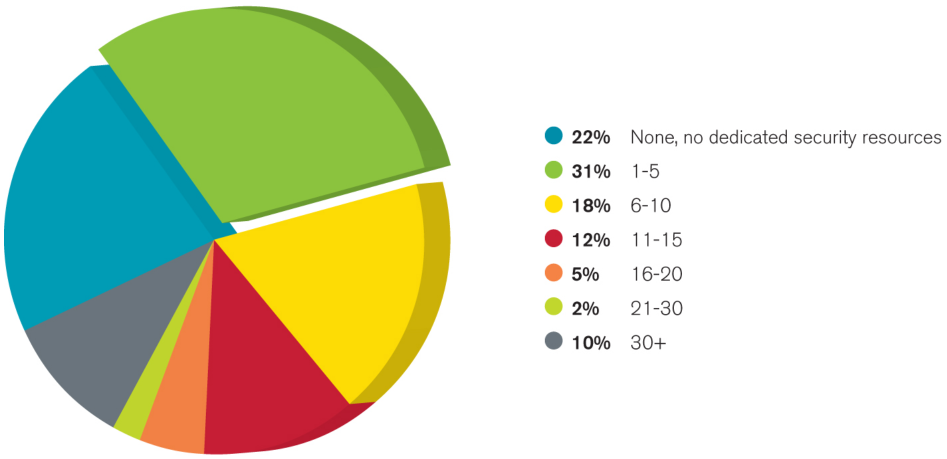


Source: Arbor Networks, Inc.

- Traffic floods and DDoS have moved up to the top spot here.
  - May indicate more focus on the availability of IPv6 services from respondents
  - Big drop in percentage of respondents who would NOT mitigate an attack against an IPv6 service backs this up, change from 20% to 3.9%
- Inadequate feature parity, last year’s top concern, has moved down to third
  - This may indicate that equipment vendors have finally delivered the IPv6 feature parity they have been promising
- Visibility has dropped considerably as a concern
  - Maybe due to the improved level of flow support (63% -> 74.5%) for IPv6
- Misconfiguration remains an issue

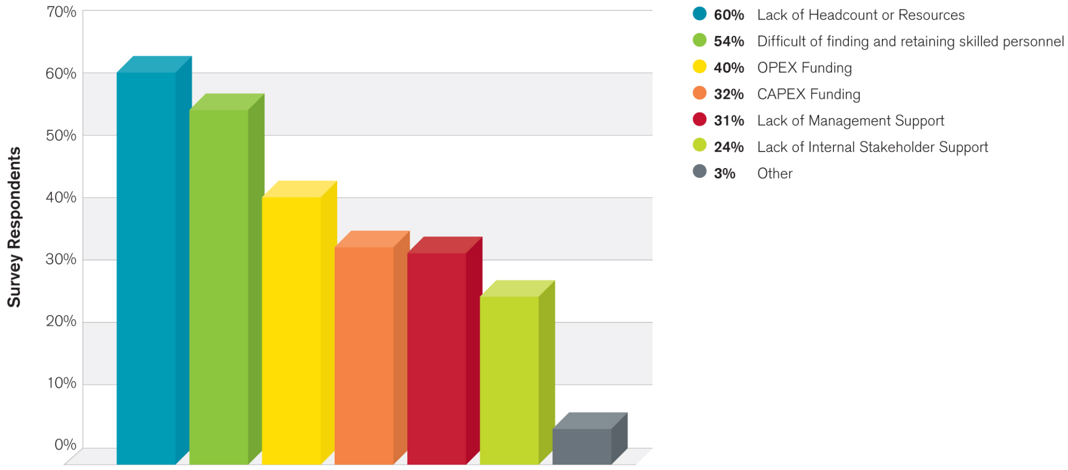
Operational Security Team Headcount

OPSEC Team Head Count



Source: Arbor Networks, Inc.

OPSEC Team Challenge

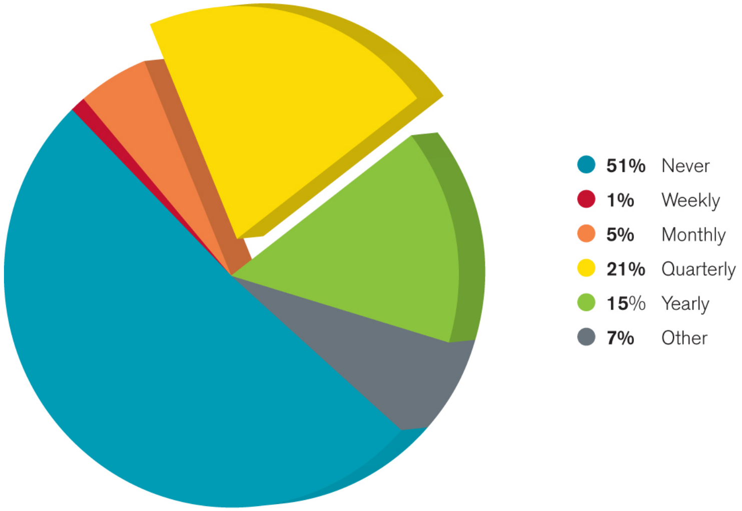


Source: Arbor Networks, Inc.

- Just under a quarter of respondents have NO dedicated security resources
  - An increase from last year. Maybe due to increased outsourcing.
- 'Lack of headcount and resources' top issue when building and maintaining a security team
  - Increase in the proportion of respondents citing Opex and Capex funding as issues this year.

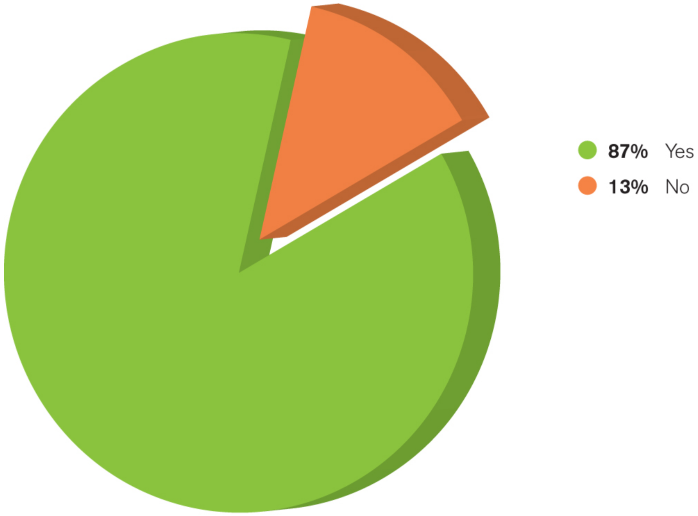
Attack / Defense Readiness

Attack and Defense Simulations



Source: Arbor Networks, Inc.

Maintaining Contact Information

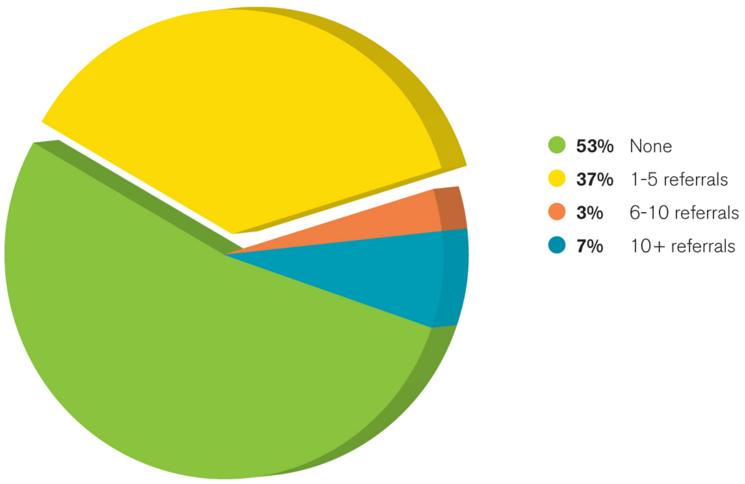


Source: Arbor Networks, Inc.

- A half of respondents NEVER practice their incident handling processes
  - Not good, but better than the 58% last year
- 86.7% now maintain contact information for their peers, transit providers etc.
  - A 17% improvement on last year
  - Security incidents can be prolonged if the right people are not involved

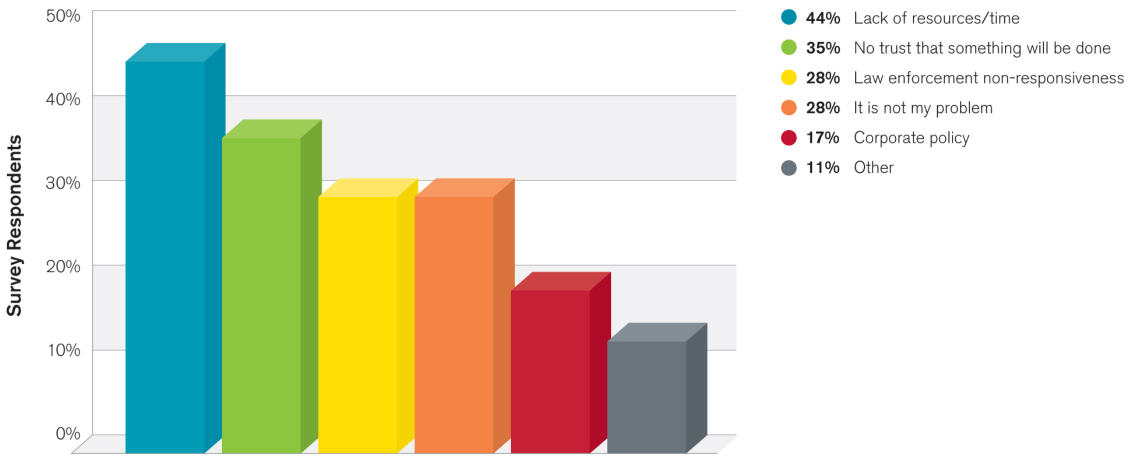
Law Enforcement Referral

Referral to Law Enforcement



Source: Arbor Networks, Inc.

Reason for Not Referring to Law Enforcement



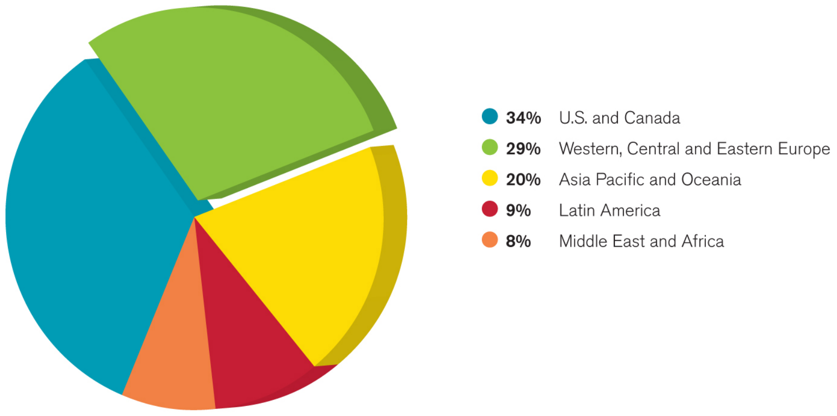
Source: Arbor Networks, Inc.

- More than half of respondents do NOT refer security incidents to law enforcement
- Biggest barriers are ‘lack or resources’ and ‘low confidence that anything will get done’
- 84% believe government CERT / CSIRT have a positive role to play and welcome their involvement

66% believe governments are NOT doing enough to protect critical infrastructure

2012 Infrastructure Survey Demographics

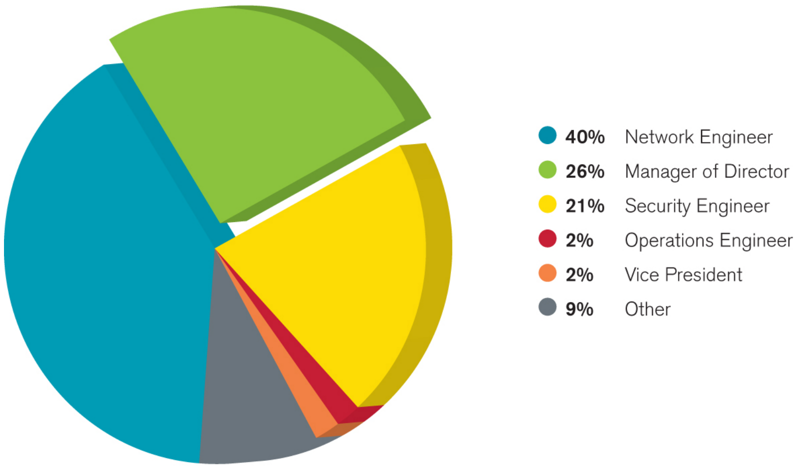
Geographic Distribution of Organizational Headquarters



Geographic distribution

- 29.1% Europe
- 34.2% US and Canada
- 9.4% Latin America
- 19.7% APAC
- 7.7% Middle East / Africa

Role of Respondent



63% of respondents network, security, operations engineers, analysts or architects

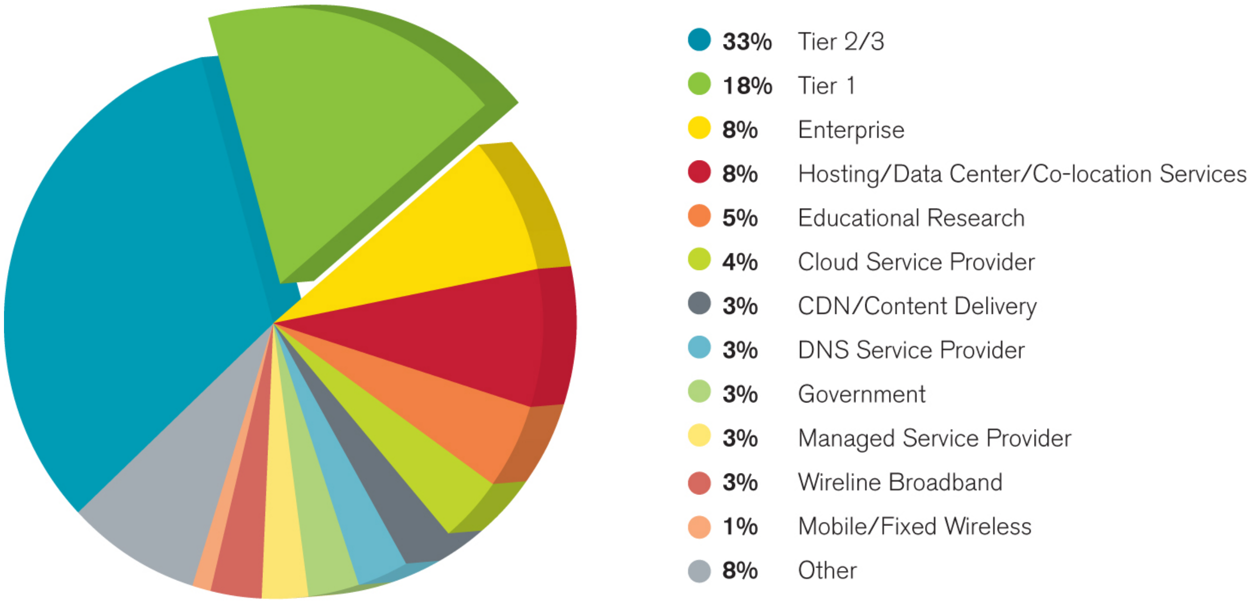
28.1% of respondents management or executives

Source: Arbor Networks, Inc.

ARBOR® NETWORKS

2012 Infrastructure Survey Demographics

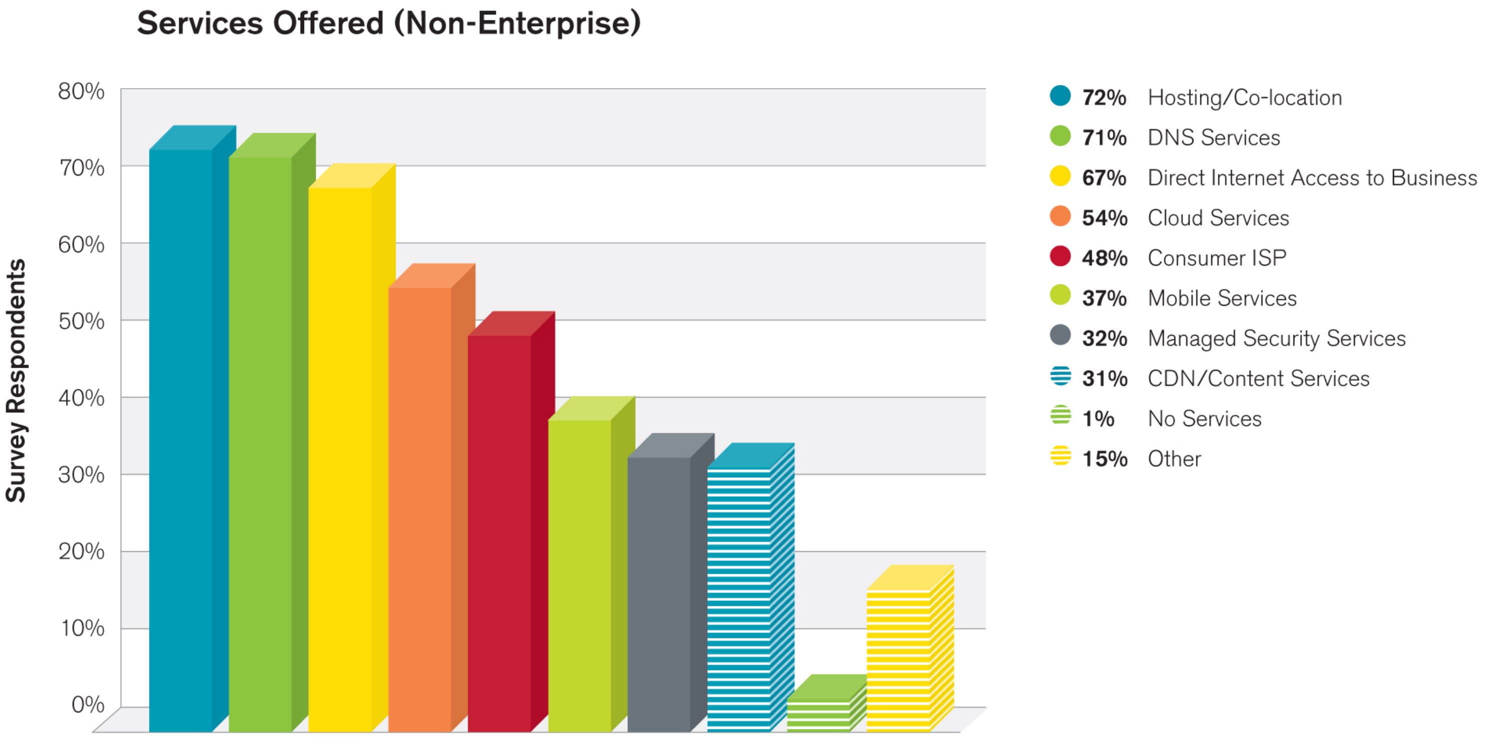
Survey Respondents by Organizational Type



Source: Arbor Networks, Inc.

- Survey conducted in September 2012 & October 2012
- 130 total respondents across different market segments
- 75% Internet Service Providers

2012 Infrastructure Survey Demographics



Source: Arbor Networks, Inc.

- Multiple services offered by most respondents
- Business Internet, Co-Location and DNS services most common
- 62.3% of respondents offer managed security services

ARBOR® NETWORKS

Thank You