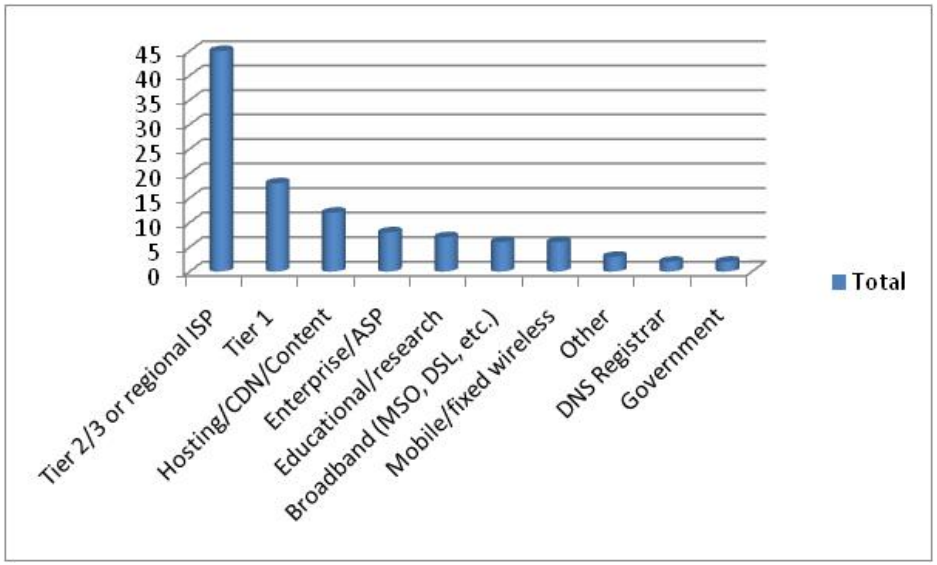
2010 Infrastructure Security Report

6th Annual Edition

Roland Dobbins
Craig Labovitz
Carlos Morales

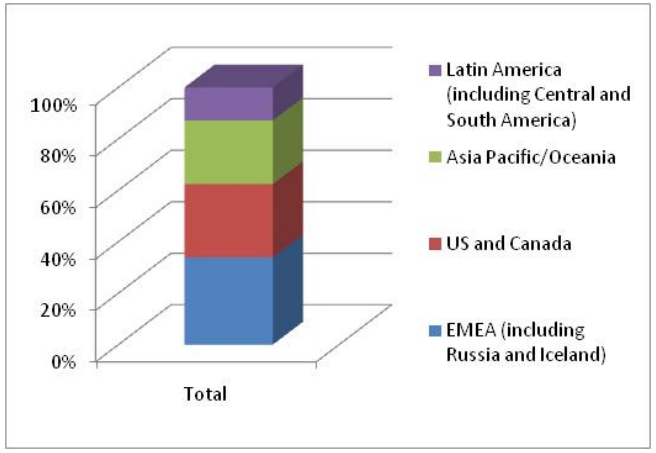
2010 Infrastructure Security Survey

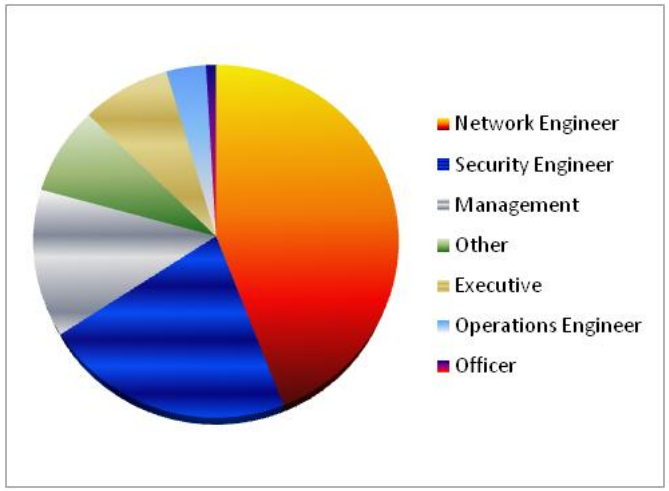
- 6th Annual Survey
- Survey conducted in September – October 2010
- 111 total respondents contributed
  - Service providers
  - Content/ASPs
  - Enterprises
  - Broadband
  - Mobile
  - DNS
  - Educational



Survey Demographics

- 57% are service providers
- Even geographic distribution
  - 33% EMEA
  - 28% US and Canada
  - 24% APAC
  - 15% Latin America
- Tier 1 participation jumped to 15% of the respondents from 5% in 2009
- 69% of respondents network, security or operations engineers
- 22% of respondents were management or executives

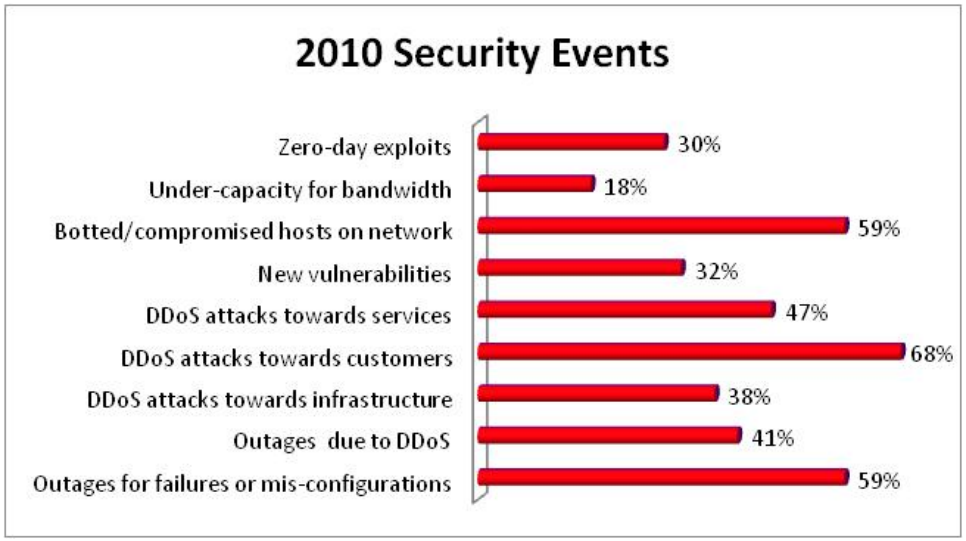


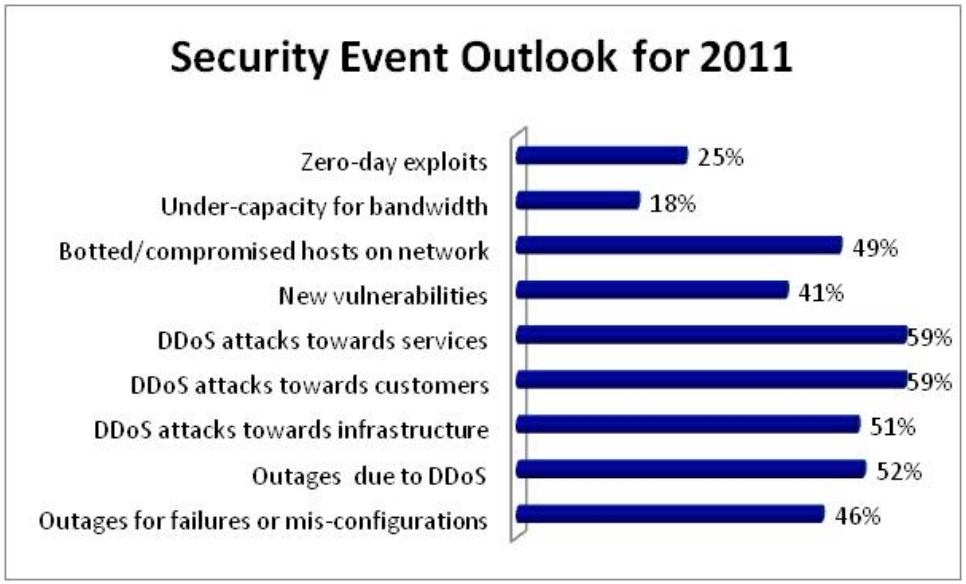


Key Findings of the Survey

- Attack surface continuing to shift
  - Attack size increases dramatically attacking underlying network infrastructure
  - Application layer attacks continue with some new applications being targeted more frequently
- DDoS attack capabilities of miscreants are outpacing the defensive measures taken by network service providers
- Firewall and IPS equipment represents critical points of failure during DDoS attacks
- DNSSEC security concerns on the rise as deployments begin and IPv6 security has become an arms war
- Mobile network growth is a game changer – availability of limitless bots with greater bandwidth and few network control points

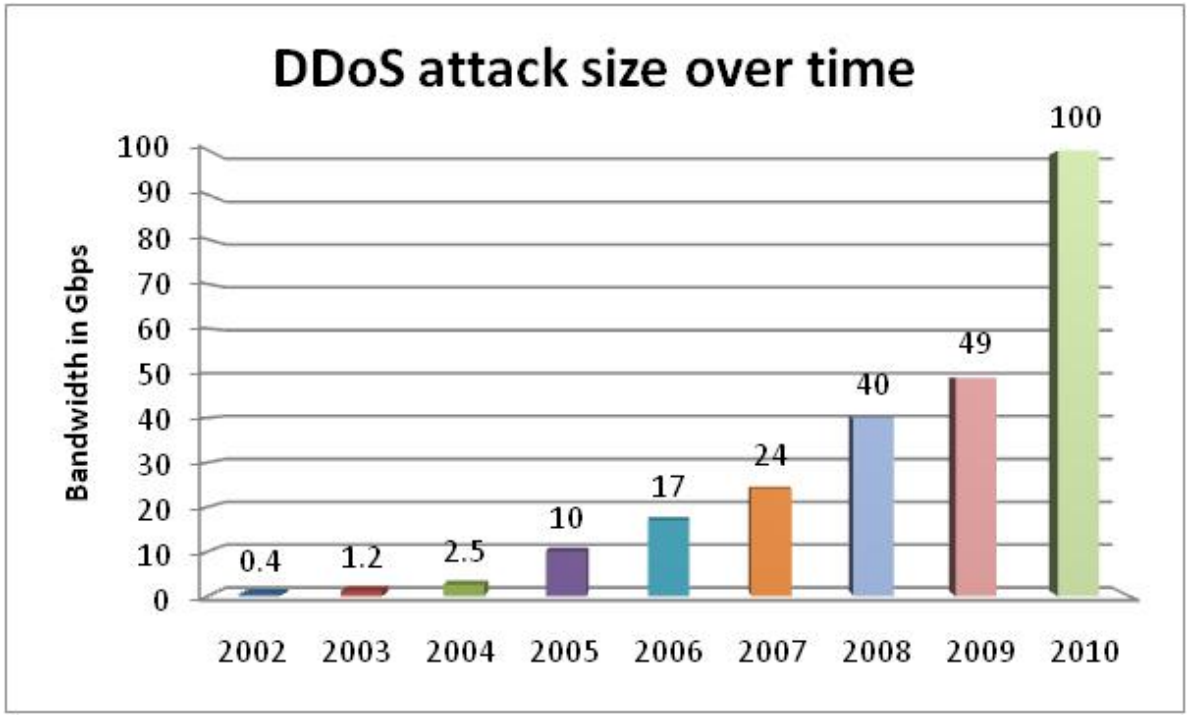
2010 security events and outlook for 2011





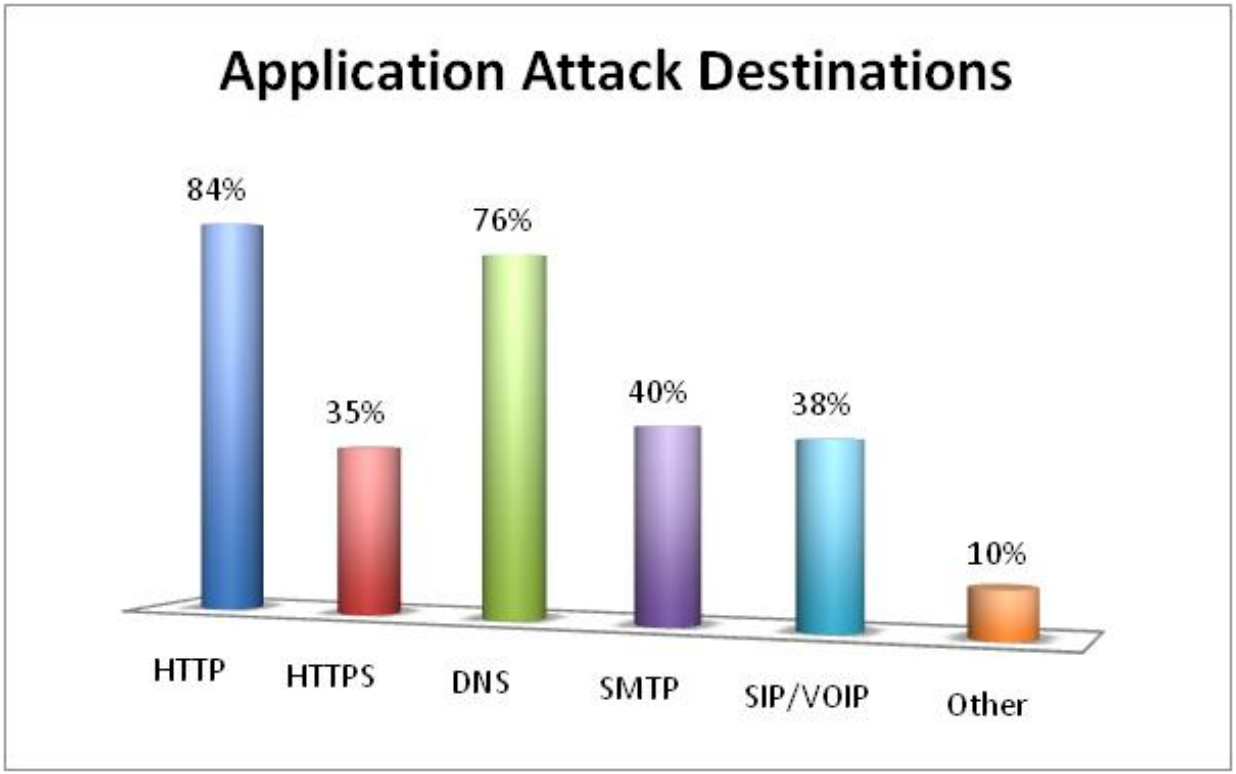
- Botted hosts and DDoS attacks against customers have been the top security targets for 2010
- Participants predict more attacks towards services and infrastructure in 2011
- Projected increase in number of outages due to DDoS in 2011 shows concern over the mechanisms in place to deal with attacks

DDoS Attack Sizes Over Time



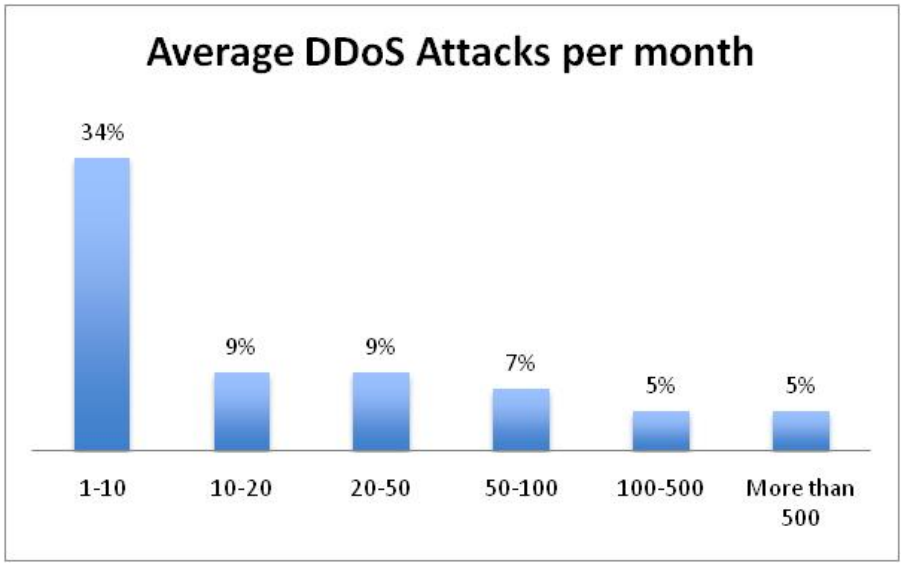
- Over 100% increase YOY in attack size shows renewed push towards volumetric attacks
- Internet providers have focused on application threats so miscreants turned back towards attacking network capacity

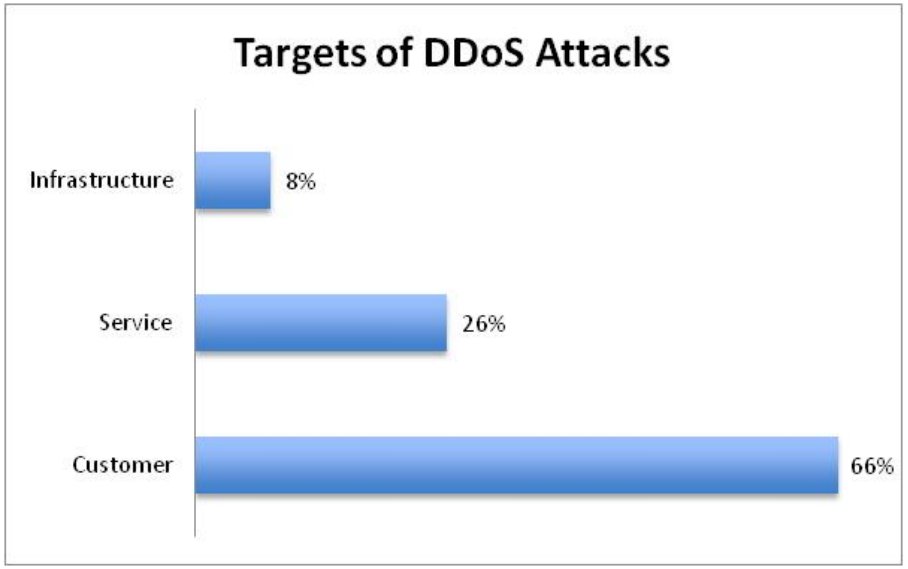
Application Layer Attacks



- 77% of respondents detected application layer attacks so this continues to be a major attack vector
- HTTP and DNS remain the top targets but HTTPS, SMTP and SIP/VOIP attacks are becoming more common

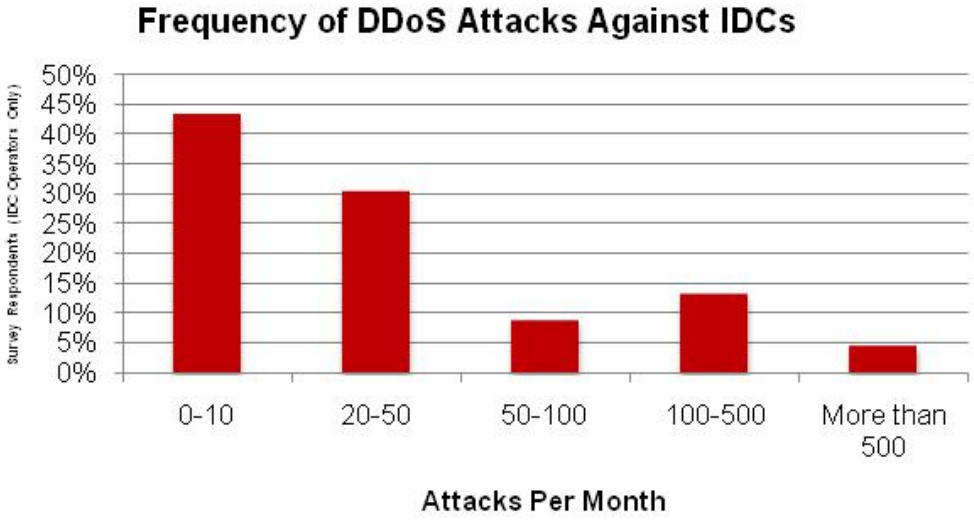
Attack Frequency and Targets

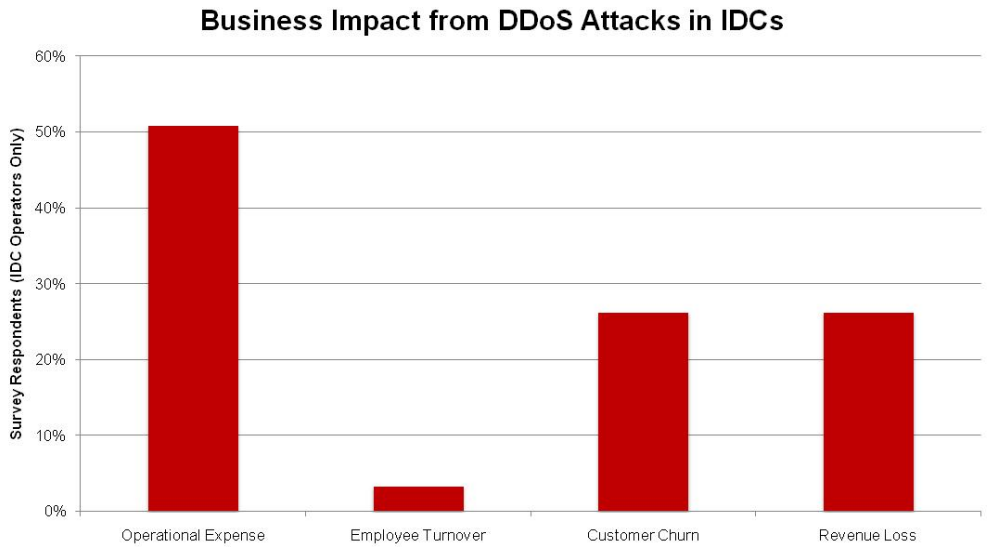




- Attack frequency is increasing
  - 76% of respondents see at least 1 DDoS attack per month
  - 35% of respondents see 10 or more DDoS attacks per month compared to 18% in 2009
- The majority of the attacks are specifically targeted at customers or services
  - Size of attacks will still cause much collateral damage

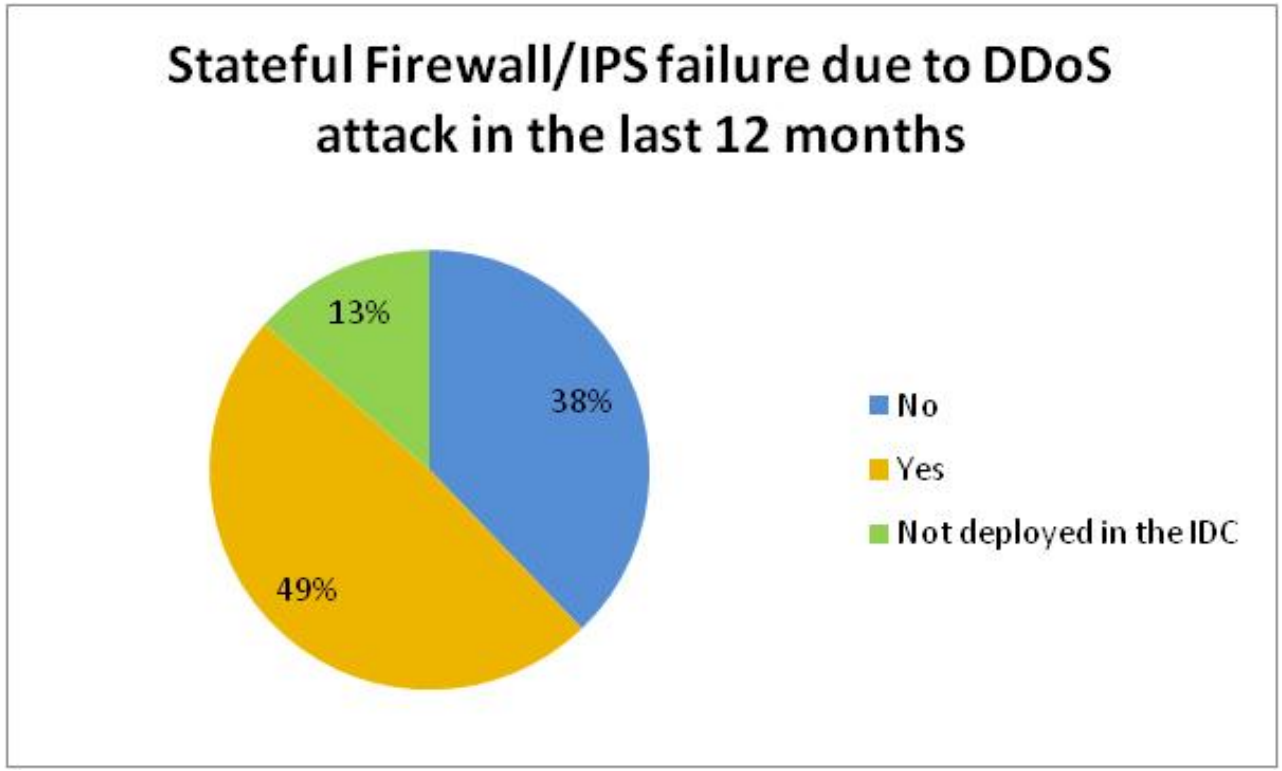
Impact of attacks against IDCs





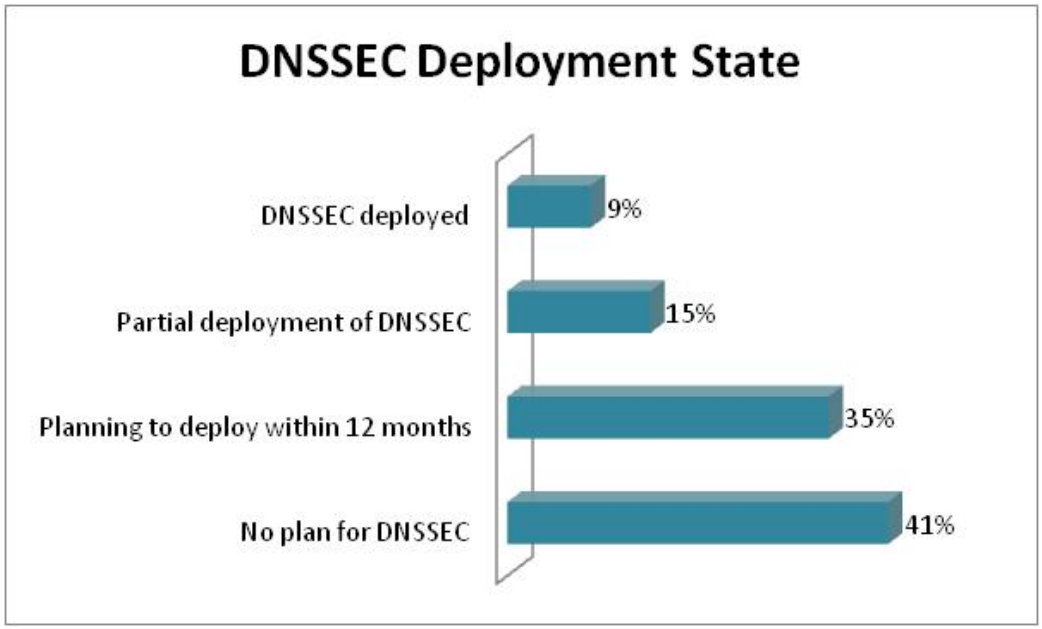
- Attack frequency varies quite a bit by respondent
- Some have seen a dramatic number of attacks
- Huge impacts in operational expenses, revenue loss and customer churn result from attack

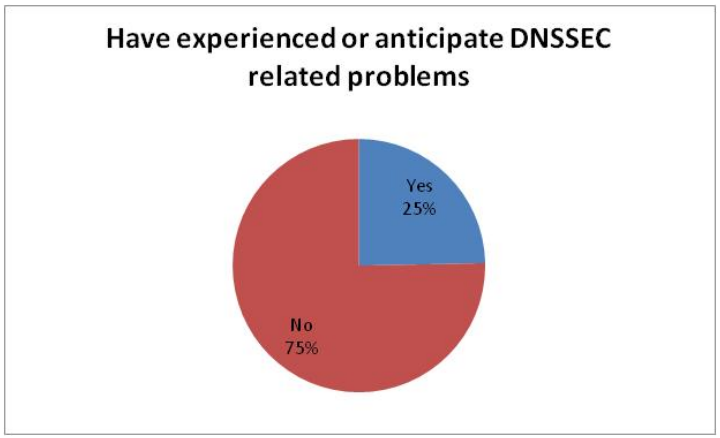
Failure of Firewall and IPS in the IDC

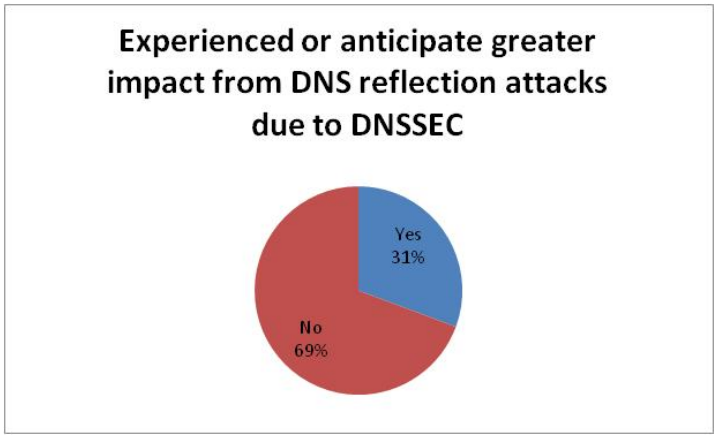


- **Nearly half of all respondents have experienced a failure of their firewalls or IPS due to DDoS attack**

DNSSEC Threats

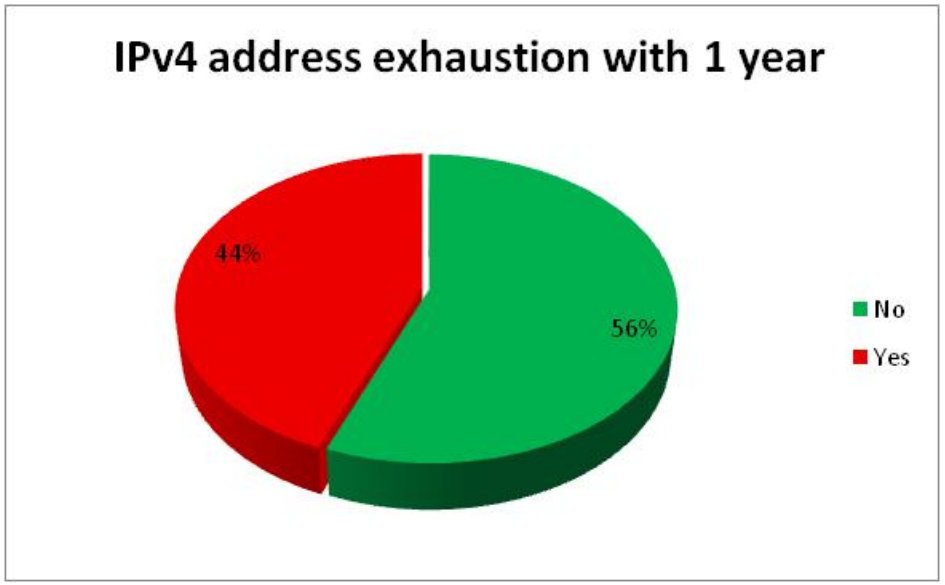






- 25% of respondents have deployed DNSSEC
- Already 25% have experienced or expect problems and 31% expect increase in amplification

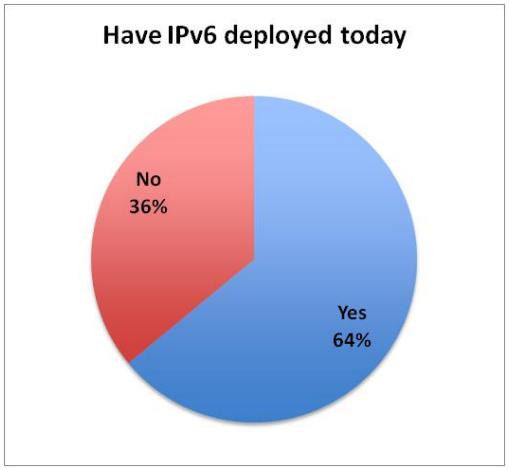
IPv4 Address Exhaustion

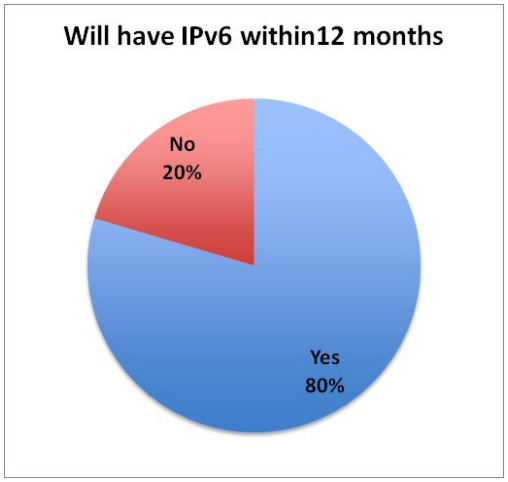


- 44% of participants predict that they will be exhausting their IPv4 allocations within the next 12 months
- With the overall industry exhaustion of IPv4 space, this may lead to business continuity concerns
  - Network architectures will need to be examined
  - More NAT/PAT use
  - Faster migration to IPv6

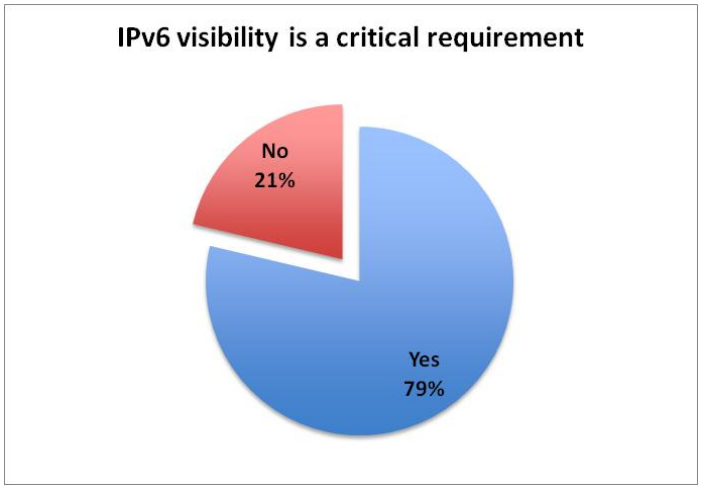
Deployed IPv6 is growing

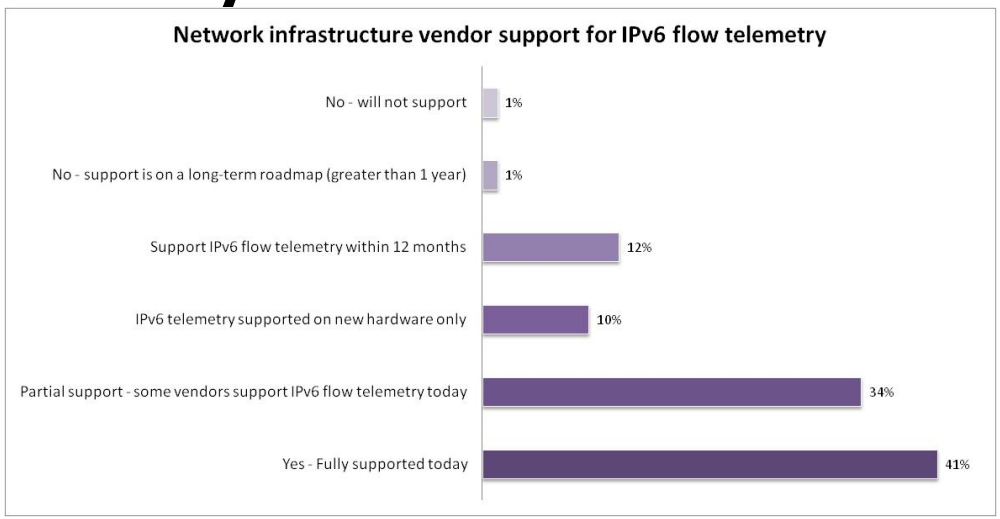
- 64% of respondents already have IPv6 deployed to a limited extent and 80% of respondents expect to have IPv6 deployed within 12 months
- 500Mbps is the peak today but major growth is expected with IPv4 address exhaustion
- Can security teams keep

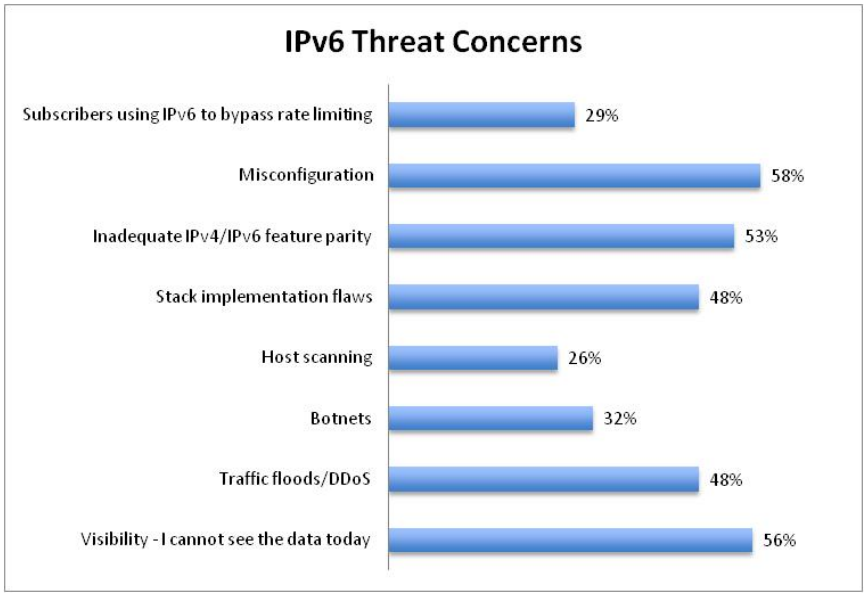




The IPv6 Security Arms War

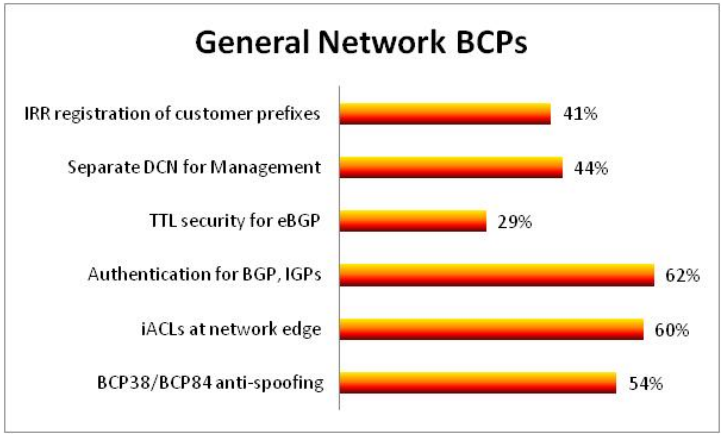


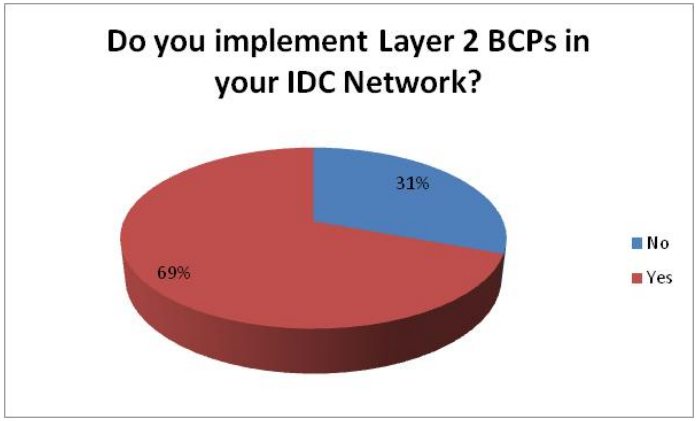


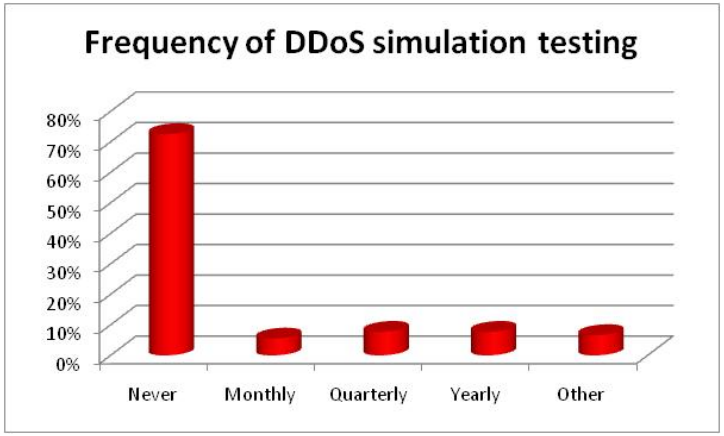


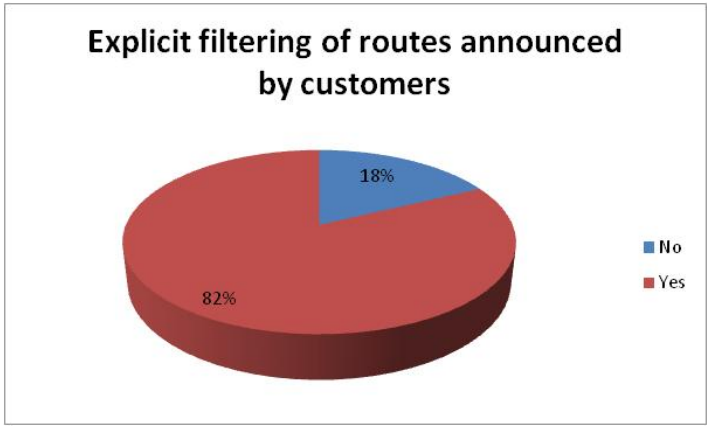
- Vendors and network operators are rushing to introduce IPv6 visibility and security as networks scale up

Security Best Current Practices (BCPs) Utilized



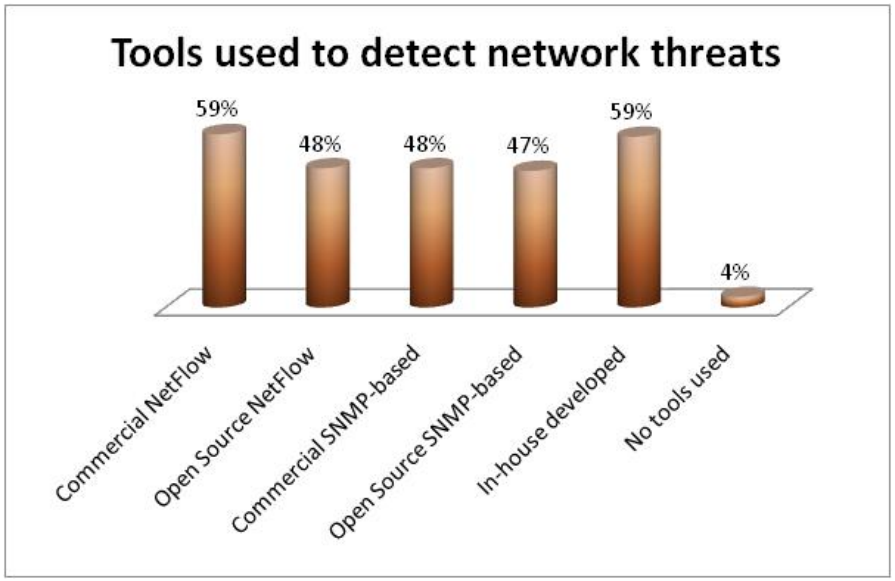


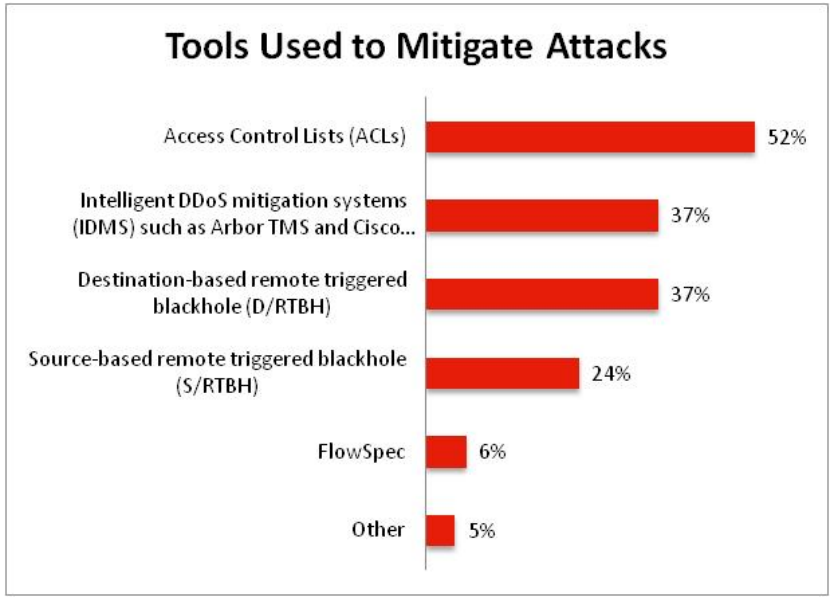




- **More than 2/3 of respondents are implementing some BCPs**
- **Preparation of operators to deal with threats is lacking**

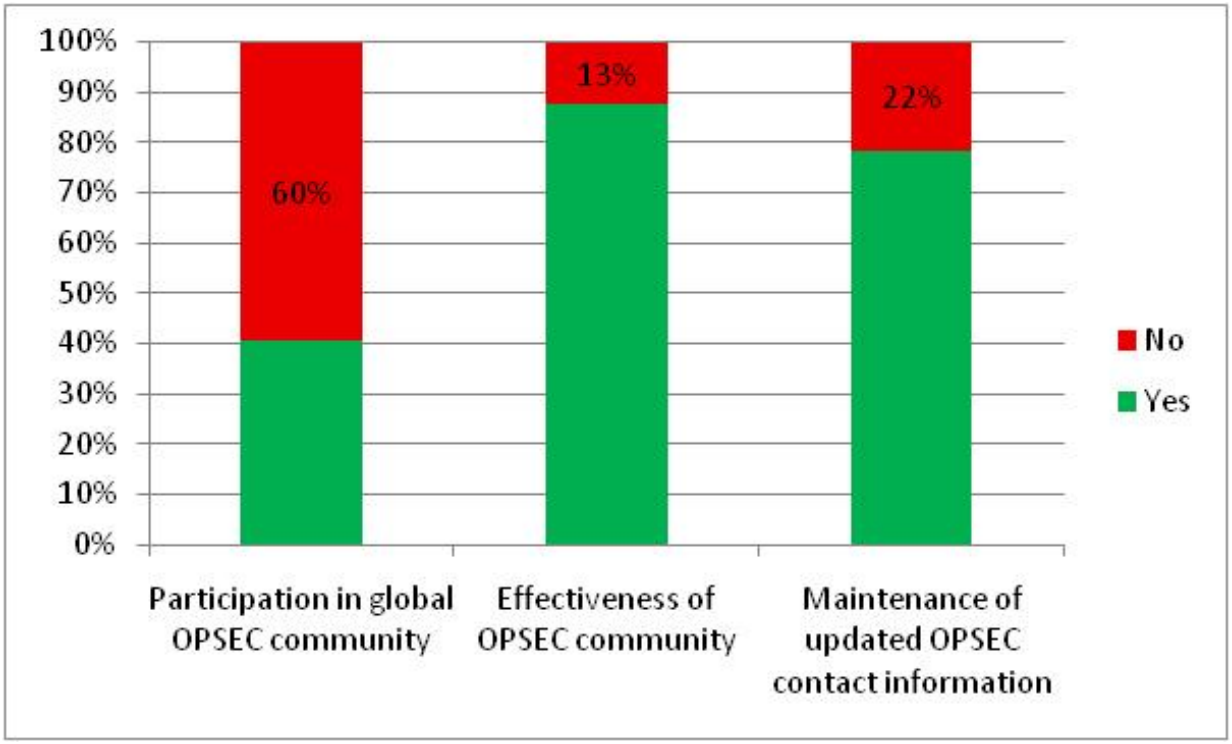
Tools Used for Threat Detection and Mitigation





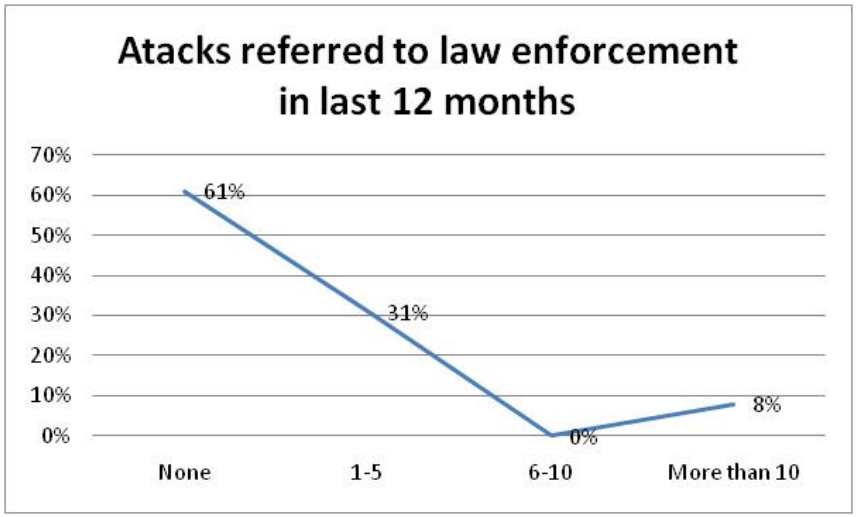
- 96% of the respondents had some means of detecting DDoS threats but only 72% had used any form of mitigation
- Use of intelligent DDoS mitigation systems (IDMS) increased from 18% in 2009 to 37% in 2010

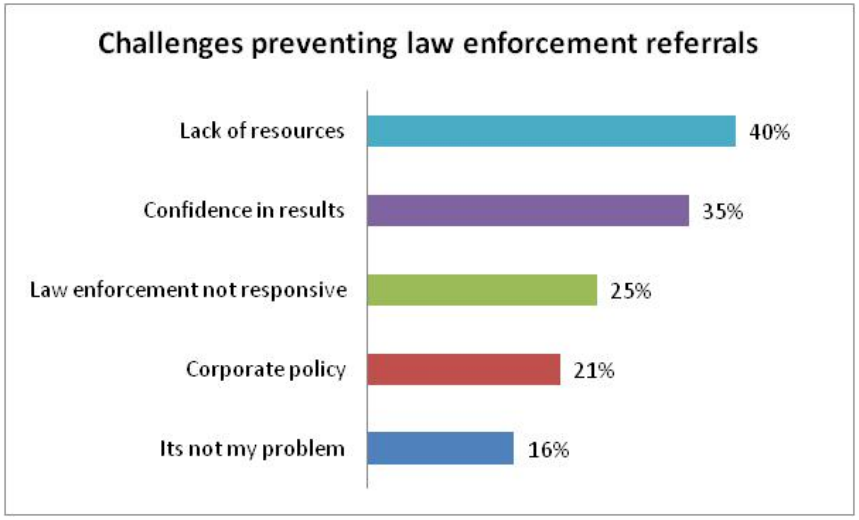
Global OPSEC Community Participation

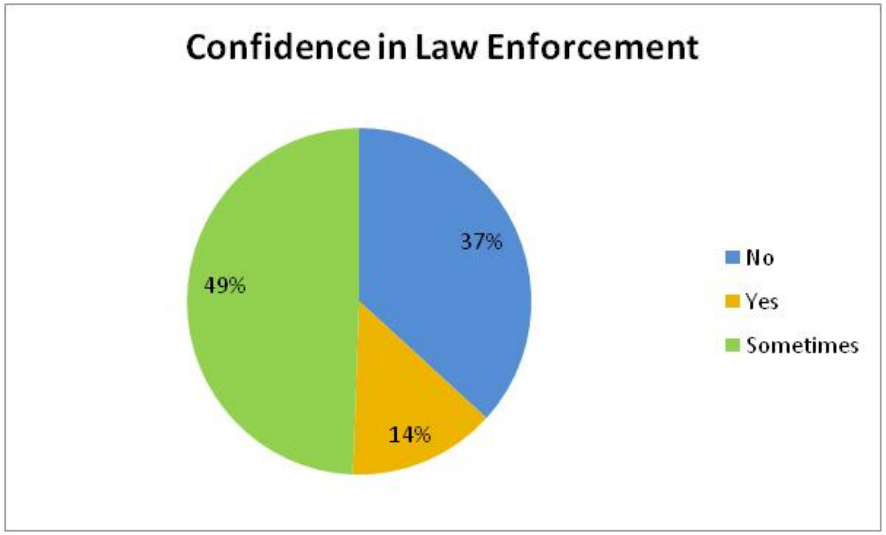


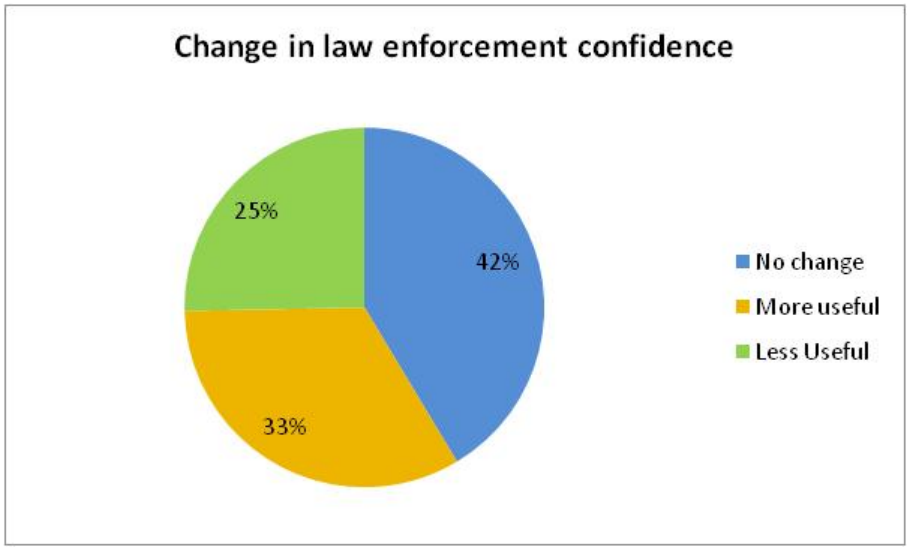
- **It is generally agreed that the global OPSEC community is useful in helping to mitigate security incidents and most participants have the means to contact them**
- **Low participation in the OPSEC community is mainly due to too few resources available to deal with threats**

Confidence in Law Enforcement Remains Low









Thank You