APNIC’s Engagement on Security

Geoff Huston

Chief Scientist, APNIC

Even simple machinery can fail in epic ways!

With more complex machinery…

We can confidently anticipate even more epic forms of failure

Our Shared Vulnerability

Many aspects of our society now rests upon digital foundations:

- Government
- Infrastructure
- Finance
- Health
- Food
- Water

If we undermine the integrity and security of these digital foundations then we expose ourselves to very serious risks

A Toxic Internet

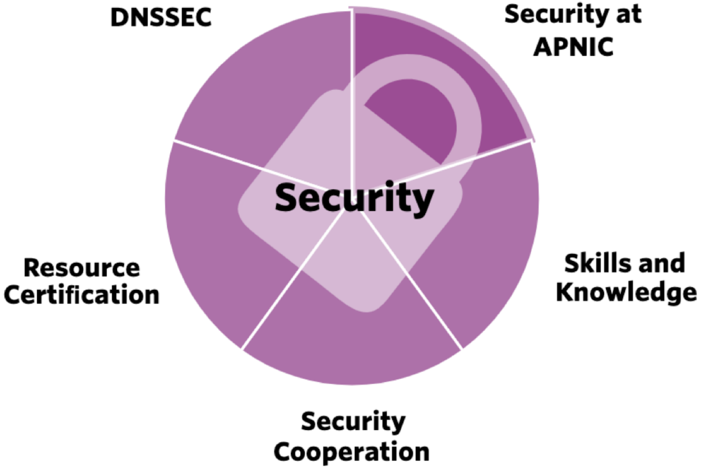
What kind of world have we built when millions of webcam baby monitors can be orchestrated to perform a terabit attack on the domain name infrastructure on the US eastern seaboard, and disrupt the lives of millions of people for an afternoon?

What are we doing about it?

APNIC’s Security Stance

APNIC’s vision is for a global, open, stable,
and **secure** Internet that serves the entire Asia Pacific community.

Security at APNIC

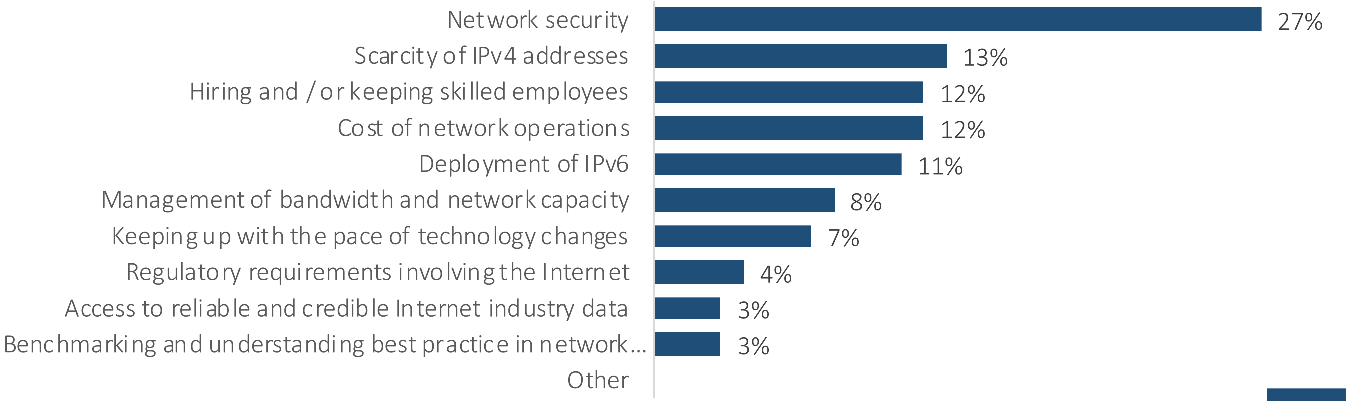


Our Surveys

- We regularly survey our members and stakeholders regarding their views of current challenges
- Security is now the highest rated challenge (it used to be IPv6)

APNIC Survey 2018

Q9. Thinking about your Internet-related services, products or activities, what are the MAIN operational challenges facing your organisation?

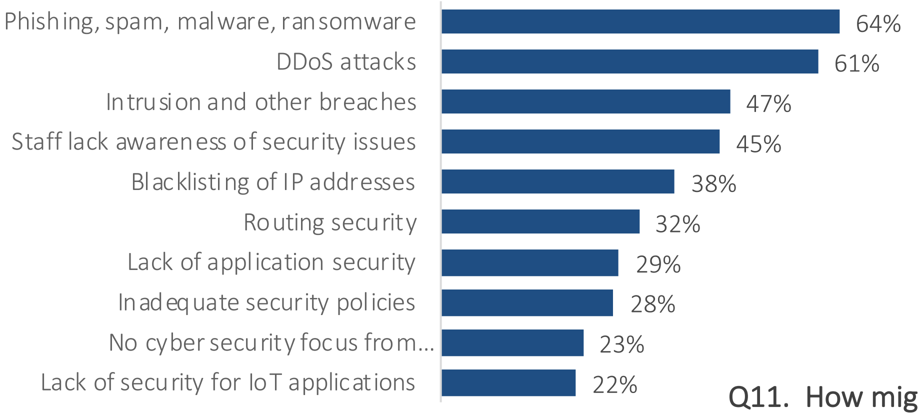


Consistent with focus group feedback, network security is the **number one** challenge facing the community in 2018

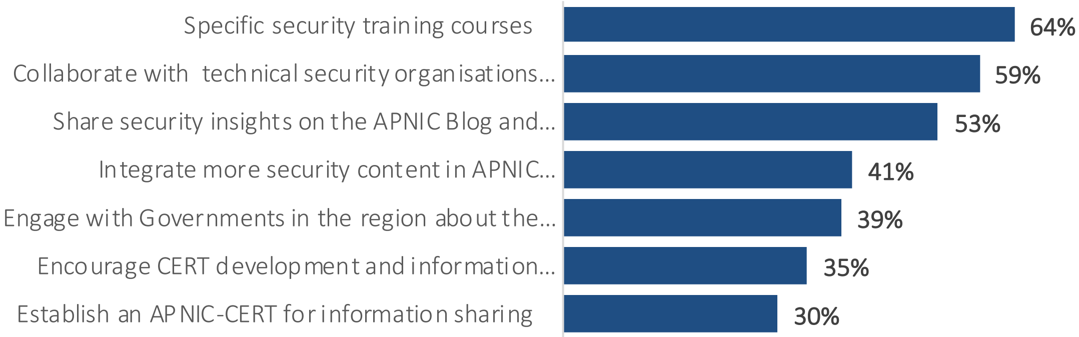
	East Asia	Oceania	SE Asia	South Asia	LDEs	Developing	Developed
Network security	28%	34%	22%	26%	28%	25%	31%
Scarcity of IPv4 addresses	13%	9%	14%	14%	11%	13%	12%
Cost of network operations	10%	14%	17%	11%	13%	13%	11%
Hiring and / or keeping skilled employees	12%	12%	13%	10%	8%	11%	16%
Deployment of IPv6	9%	8%	8%	17%	16%	10%	7%
Management of bandwidth and network capacity	9%	9%	9%	8%	7%	9%	8%
Keeping up with the pace of technology changes	10%	5%	7%	6%	5%	9%	4%
Regulatory requirements involving the Internet	4%	6%	4%	3%	4%	4%	5%
Benchmarking and understanding best practice in network operations	4%	2%	3%	3%	3%	4%	3%
Access to reliable and credible Internet industry data	3%	1%	4%	3%	4%	2%	2%
Other	0%	1%	0%	0%	0%	0%	1%

APNIC Survey 2018

Q10. Thinking about network security, what are the MAIN challenges facing your organisation?



Q11. How might APNIC best assist you or others with network security challenges?



What we do in this area

- Sharing global security best practice information with APNIC Members and building regional security capacity through training and technical assistance
- Working with the NIRs to ensure accuracy of registry
  - Ongoing consistency checks to historical NIR block assignments
  - RDAP and Whois alignment
  - Point of Contact validation
- Supporting the creation of CERT/CSIRTs in the Asia Pacific to strengthen the community's ability to mitigate security incidents
- Coordinating with the Asia Pacific security community, including the law enforcement community, to enhance mutual understanding and share views from the numbers community.

Infrastructure Security

- This is perhaps the most critical common vulnerability in the Internet
- If an attacker can successfully undermine the integrity of the routed address space and the integrity of the name space then the attacker does not have to target individual hosts or systems, as the entire network is exposed

Infrastructure Security

- How can we improve the name and address infrastructure of the Internet to mitigate the continual stream of routing anomalies and name hijacks?
  - Some collection of cryptographic mechanisms appears to offer the most promise, by allowing all BGP speakers and DNS resolvers the ability to distinguish a genuine artefact from an artifice intended to mislead and misdirect

Securing the Address Space and Routing

- Some 15 years ago APNIC designed a secure framework that allows testable attestations about addresses and their uses – this is today's RPKI
- We've been working with other RIRs, the IETF, the Internet Society and other stakeholders to encourage the use of this RPKI as a the central tool to support address and routing integrity
- We continue to work in the IETF for viable approaches to integrate this RPKI into the inter-domain routing system

Securing the DNS

- We are supporting the effort to deploy DNSSEC validation across the resolution space
- We are using measurement platforms to inform the community what is happening with DNSSEC deployment, and encouraging service operators to switch on DNSSEC validation
- We have encouraged DNS resolver vendors to integrate DNS features that make the DNS more resilient against attack and reduce the fragility of the current WebPKI CA system

We are doing what we can here

- But its probably not enough when thinking about the scope of the security issues confronting us
- There is no magic solution in our visible future, so we don’t expect this topic to go away anytime soon
- While there is no ‘silver bullet’ to make all this just go away, we are doing what we can, and working with others, to make incremental improvements in the area, to make abuse and attack more challenging for bad actors