

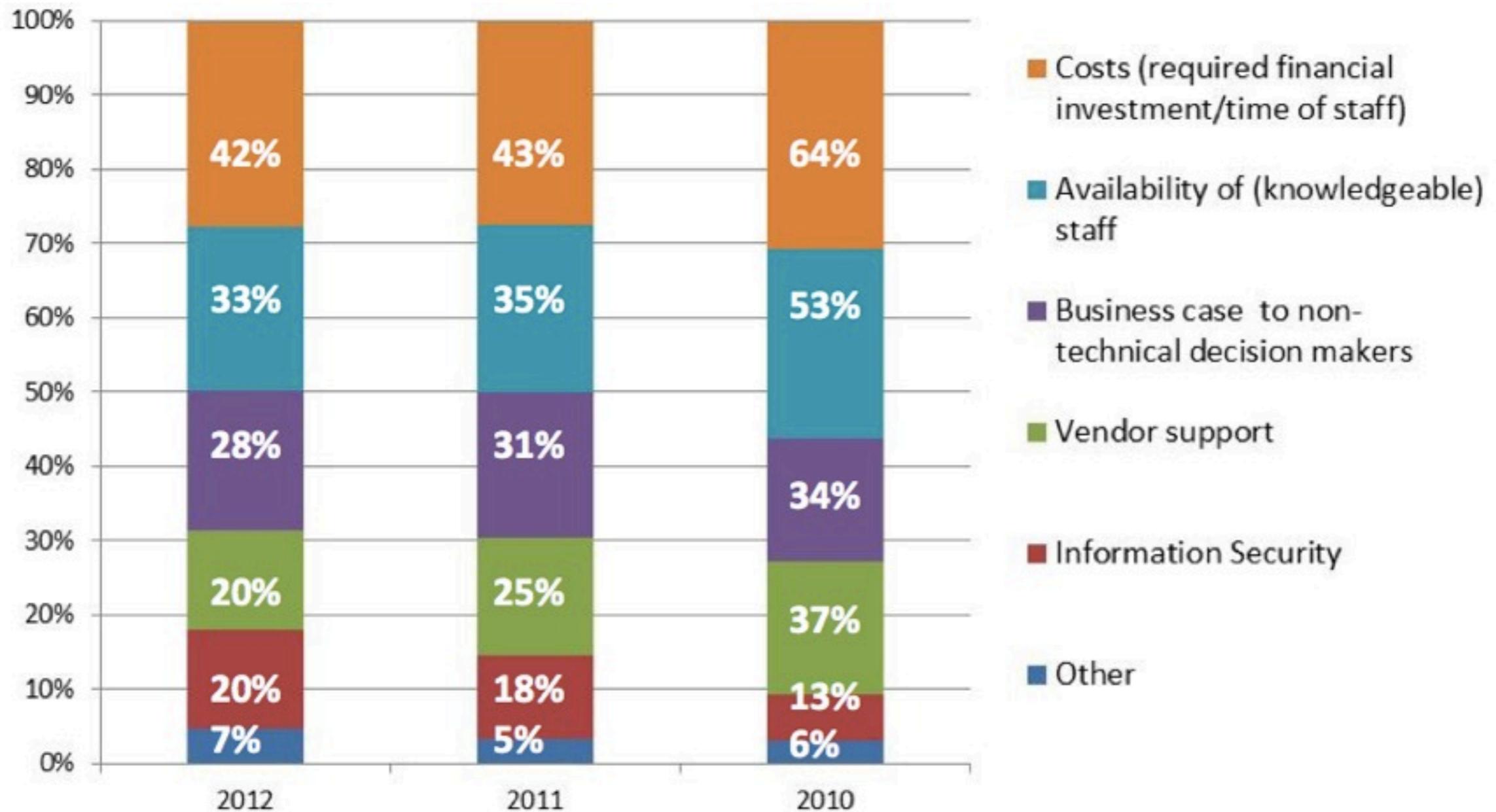
IPv6 Security

Where is the challenge?

Marco Hogewoning
External Relations
RIPE NCC



Biggest Hurdle Deploying IPv6



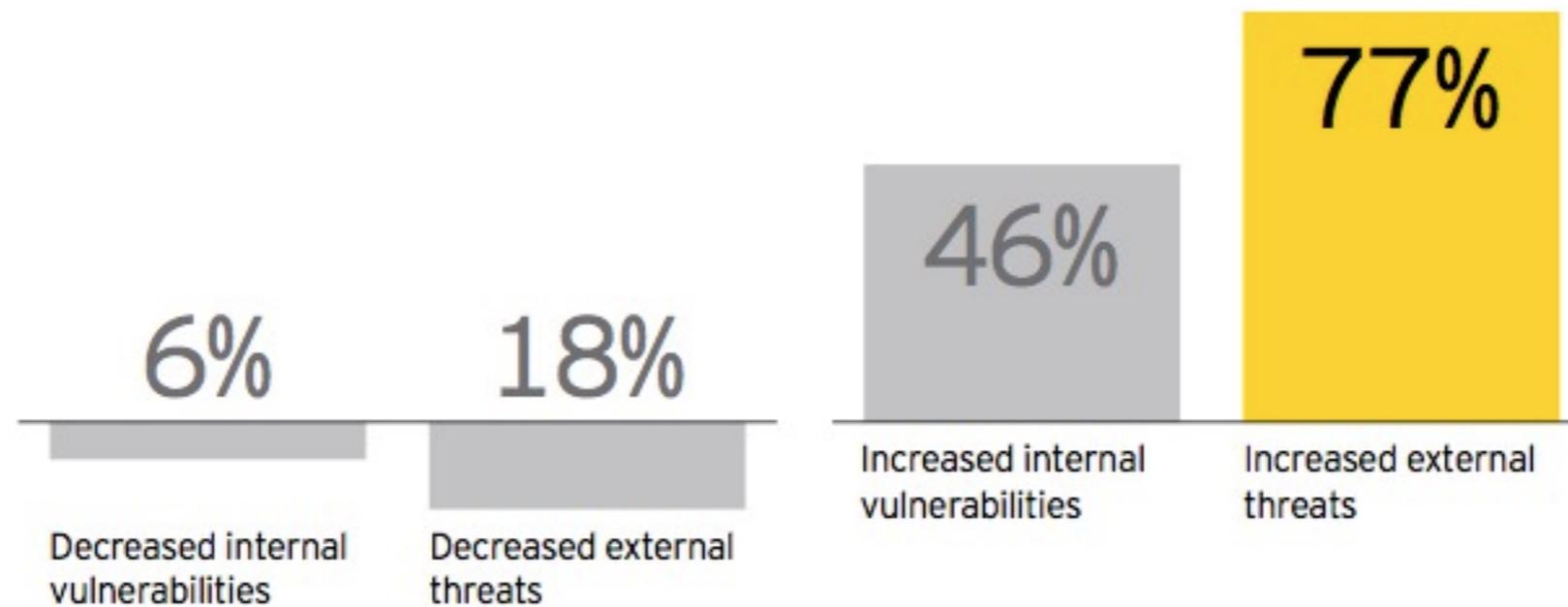
(NRO: Global IPv6 Deployment Survey)

Increased Awareness?

Change in the risk environment in the last 12 months

Decreasing level of risk due to:

Increasing level of risk due to:



(Ernst & Young: Global Information Security Survey)

Where is the Risk?



Threat or Vulnerability?

- **Threat:** the potential to cause harm
 - DoS, unauthorised access, viruses
- **Vulnerability:** a weakness that can be exploited
 - Bugs, configuration errors, design flaws
- **Risk:** the possibility that a vulnerability will be exploited by somebody to cause harm

Human Factor

- Vulnerabilities exist because of human errors:
 - Coding errors
 - Configuration errors
 - Design flaws
- Doesn't mean it is **your** fault
 - But a lot of times you can limit the risk

Examples

Is this IPv6 related?



Rogue Router Advertisement

- IPv6 relies on routers to announce themselves using ICMPv6 multicasts
- Protocol has little to no security
- Every machine can claim to be a router
 - Reconfigure clients to another subnet
 - Redirect or intercept traffic

Rogue Router Advertisement (IPv4)

- Every machine can start a DHCP server
 - Reconfigure clients to another subnet
 - Redirect or intercept traffic
 - NAT44 makes it much easier to hide it
- ARP spoofing
 - Pretend I am **the** router by claiming its MAC address

Protection at Protocol Layer

- “RA Guard” feature
 - Filter route announcements on switches
 - On all ports except for the known router
 - Present in a lot of equipment already
- SEcure Neighbor Discovery (SEND)
 - Fix the protocol by adding verification
 - Add cryptographic certificates and signatures
 - **No widespread implementation**

What About Layer 2?

- Securing access to the physical network:
 - 802.1x authentication
 - Disable unused ports on switches
 - Strengthen wireless passwords
 - MAC address counters or filters (port security)
- Lowers the risk for both protocols
 - Can protect for other vulnerabilities

Upper Layers

Where are you?



Vulnerabilities are Everywhere

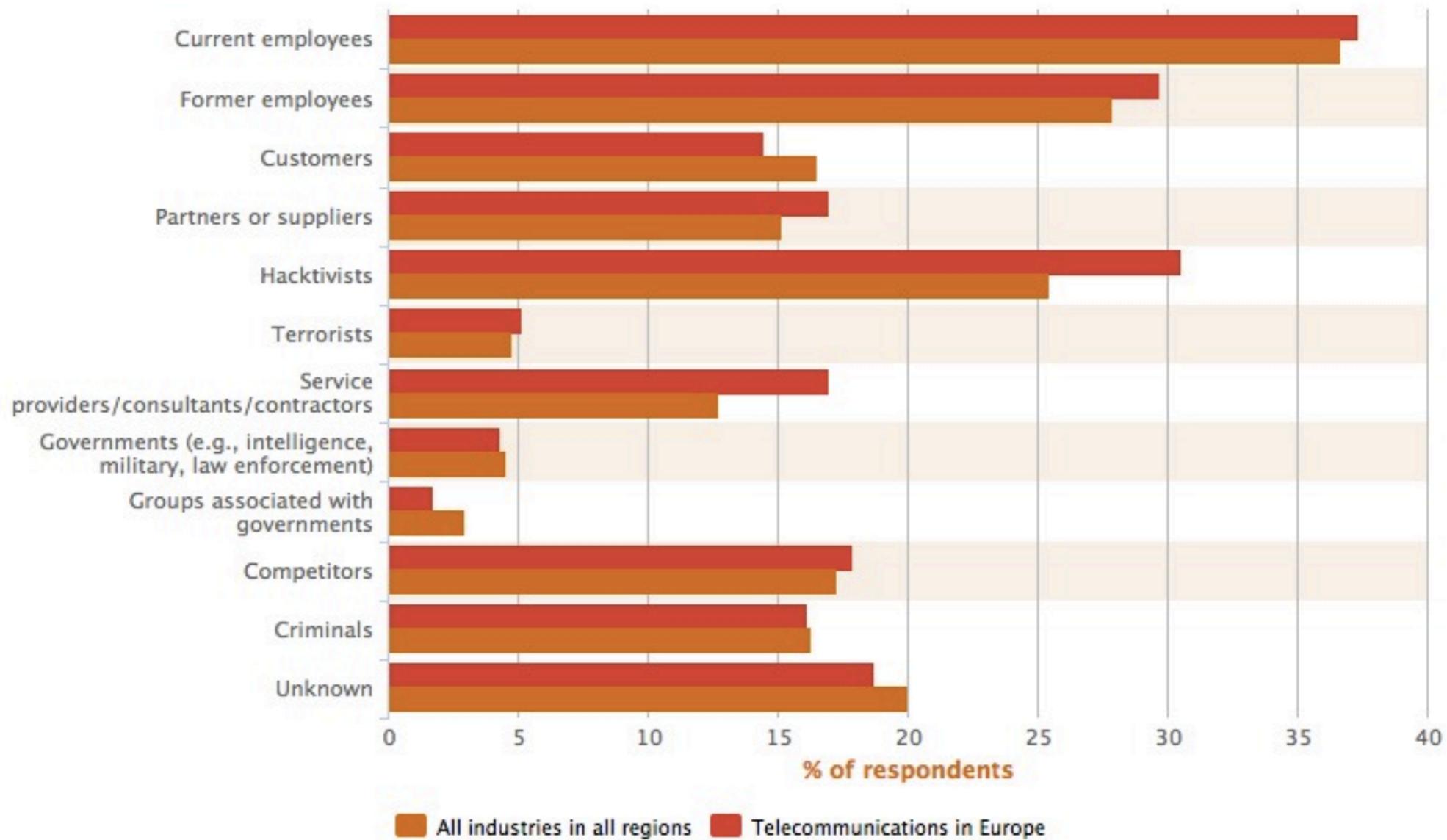
- Most security incidents caused in the application layers:
 - Buffer overflows
 - SQL injection
 - Man-in-the-middle attacks
 - Weak authentication

General Prevention Methods

- Don't run any unnecessary services
- Keep up to date with software patches
- Use encryption where possible
- Use two-factor authentication
- Keep it simple

Source of Incidents

What was the estimated source of security incidents?



(PWC: Information Security Survey)

The Human Factor

- Attacks are triggered by somebody
- Known vulnerabilities are ignored
- Mistakes can and will happen

Capacity Building

- Test your implementations before deploying
 - Don't rely on the glossy brochure
- Build up knowledge
 - Learn to identify potential risks
 - Learn how to deal with them
- Make use of available resources
 - Training courses and tutorials
 - **Share your experiences**

Improving Security with IPv6

- Multiple subnets makes it easier to separate functions or people
- Lack of NAT
 - Makes everything much more visible
 - Security moves to the end hosts
 - Forces you to think
- Somebody might already use IPv6!
 - Using tunnels to hide what is going on

Conclusion

- IPv6 might add some vulnerabilities
- IPv6 is not a threat
- You are the biggest risk

Questions?

marcoh@ripe.net

