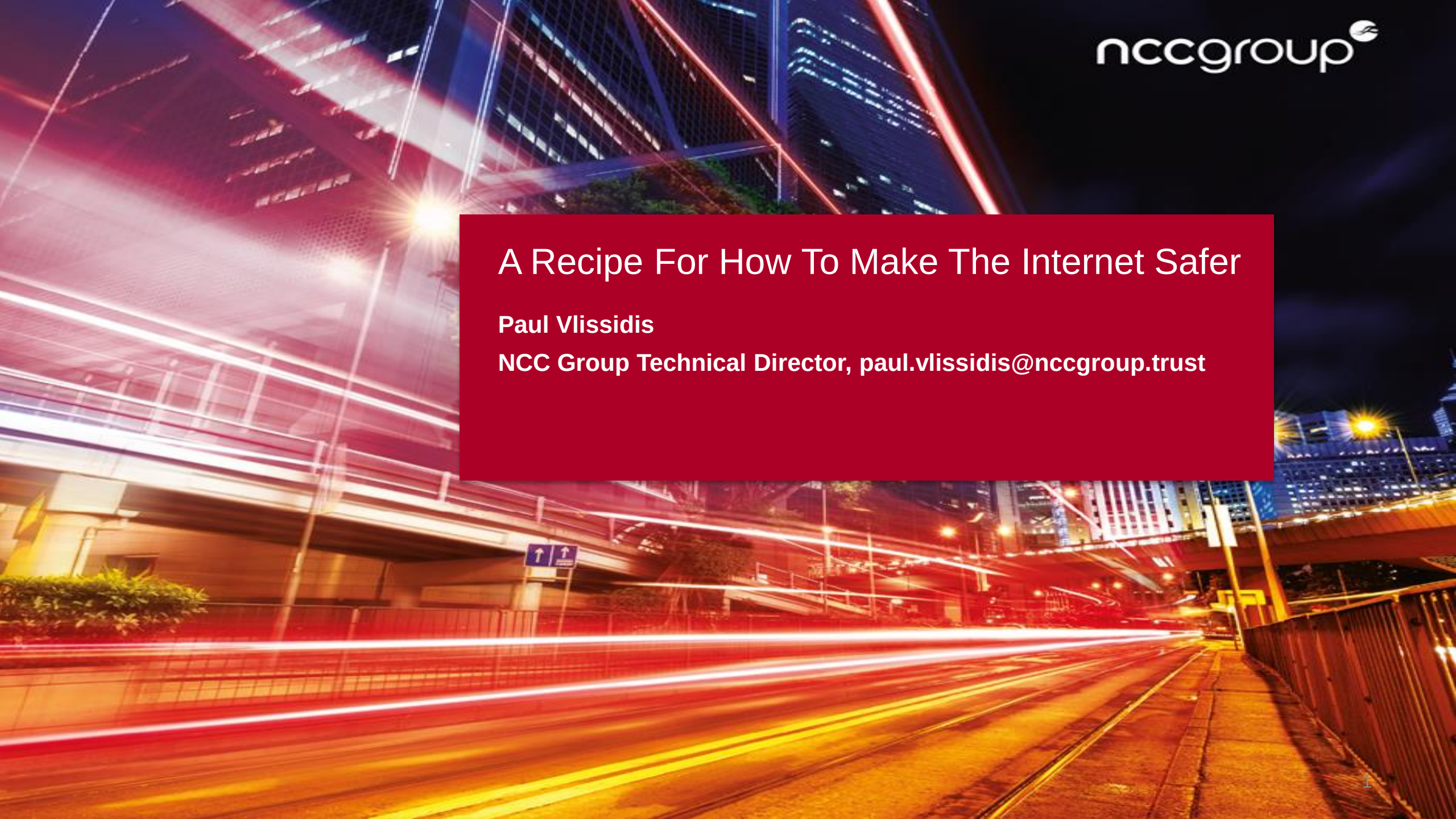


A Recipe For How To Make The Internet Safer

Paul Vlissidis

NCC Group Technical Director, paul.vlissidis@nccgroup.trust

The New Internet

Changes

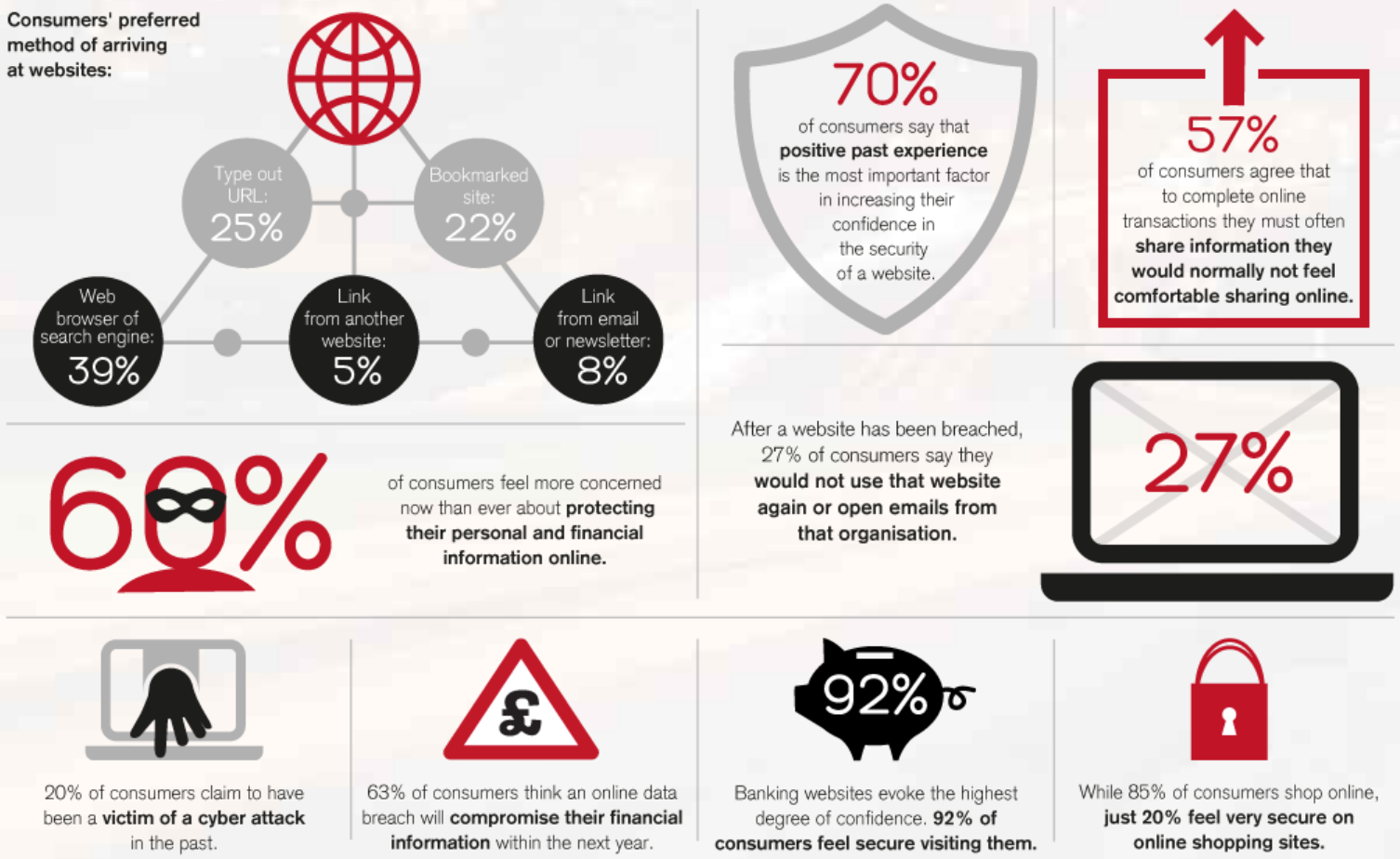
- During the next five years the Internet will transition from 1980's technologies to ones ready for the 21st century
- IPv6, DNSSEC, Software Defined Networks, IoT
- 900+ gTLDs – brands such as .HSBC, .Barclays, bnpparibas, communities such as .scot and .irish
- We will vastly increase the global security debt if we don't do anything

Opportunities

- Most importantly, this period is one of malleability, where we have an opportunity to change the user experience for the better and rebuild trust
- gTLDs offer a once-in-a-generation chance to fix many of the problems

Trust in the Internet Survey 2016

IDG Research Services



https://www.nccgroup.trust/uk/about-us/resources/trust-in-the-new-internet-survey-2016-discussion-paper/

What ingredients are needed?

Verification – users need to be sure who they are interacting with online

Security – users want to know that the highest standards are being applied

Assurance – users want the comfort that vigilance is high

Verify

Registrars need to :

- **Verify registrants**
- **Use state of the art fraud checks on registrant payments**
- **Offer secure account management – such as 2FA**
- **Have procedures to prevent domain hijacking**

.trust, .bank, .ngo,

- Applicants must submit identity documentation & proof of intellectual property & naming rights to prevent misleading, abusive & malicious registrations.
- Organisations are verified so consumers know that domains are representative of the brand they know and trust.

Closed TLDs

- Customers should be confident that closed TLDs for brands will be operated by the organisation they expect to be dealing with – but will they?

Secure using specific, auditable standards

trust Technical Security Policy

18 months to produce

66 high-level compliance issues

In the public domain & monitored by Technical Advisory Board

Developed by coalition of industry & NCC Group experts

200+ technical guidelines covering network, web app, email, DNS & abuse

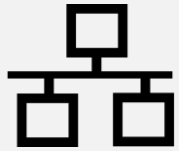
Combination of negative & positive requirements

- comprehensive
- specific
- externally verifiable
- achievable

whodoyou.trust

www.nccgroup.trust

Say what ‘good’ looks like

	Current Practice	Policy Requirement
Network 	• Insecure exposure of critical internal services is forbidden • Operating systems & services kept up-to-date on patches	• All services must be exposed only over secure channels
Web App 	• Must not have known critical web application vulnerabilities - e.g. SQL Injection, XSS, CSRF, etc.	• Implement cutting edge security standards that reduce risk and minimise attack surface. CSP. • OWASP
Email 	• None	• Publish security policy in DNS that eliminates the risk of spam from your domain • DMARC • Email must be communicated over a secure transport (TLS)
Abuse 	• “perform periodic evaluations to identify and evaluate evolving malware threats"	• No serving of or linking to malicious content – flip DNS on detection • Continuous Monitoring of domain & IP blacklists for your names and addresses
DNS 	• None	• Cryptographically signed DNS records (DNSSEC with NSEC3) • Secure registrar protected with multi-factor authentication

Assure

Policy checks, Abuse & Security Monitoring

What is being done

- Abuse monitoring of the whole TLD
- ICANN Specification 11 (rule 3(b)) requires this for all new gTLDs
- Older TLDs escape (again)

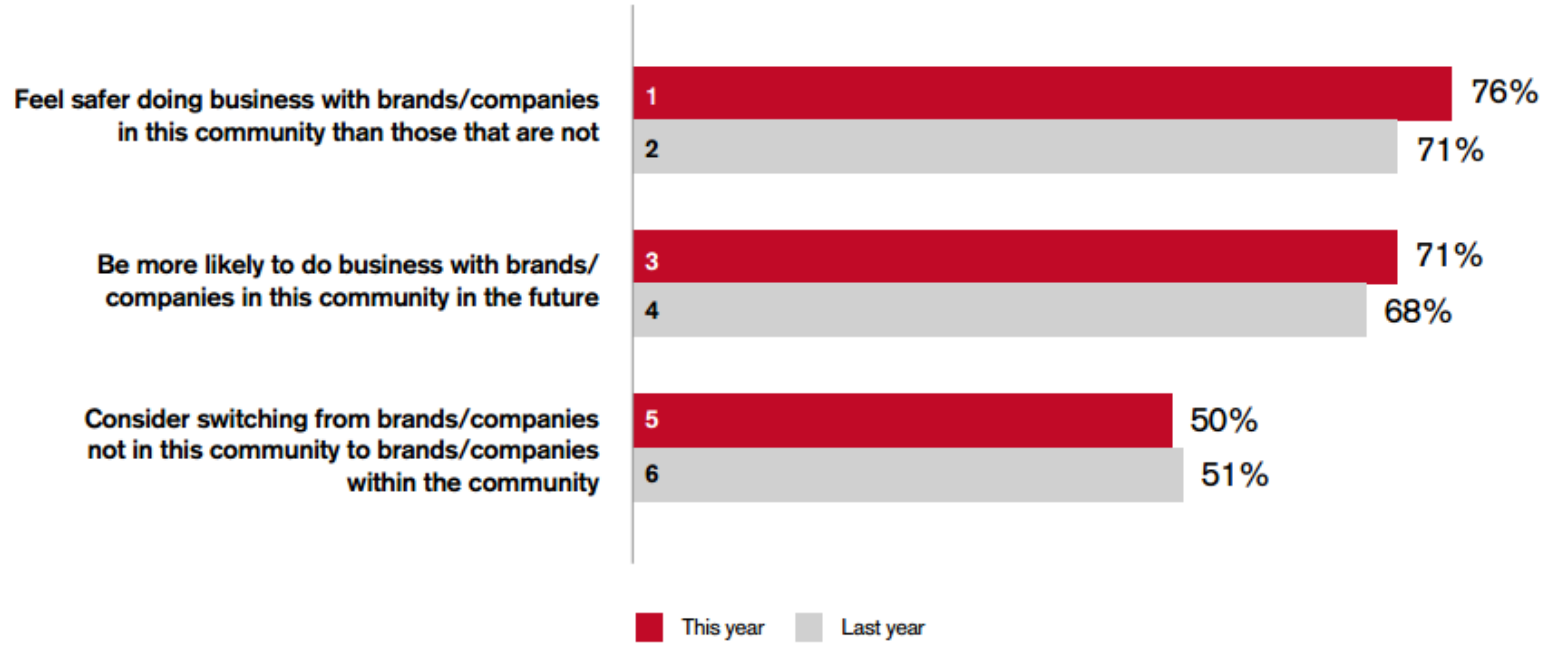
What could be done

- Every Registrant should be assessed against the TLD registry policy on domain renewal
- Registries could proactively intervene
- Registrant reputation checks during registration

Community Initiatives

- **Community Approach**
  - If we are going to make a difference then we need to form communities that commit to high standards and get onto the front foot
  - Build a community of closed TLD owners and verified domain owners
- **Education and Awareness**
  - Publicise and educate consumers through the community
  - Show people what good looks like from a security perspective
- **Vigilance**
  - Monitor communities' compliance with the agreed registry policies
  - Continuous abuse monitoring

Why it's worth doing



Source: Trust in the New Internet Survey 2016, IDG