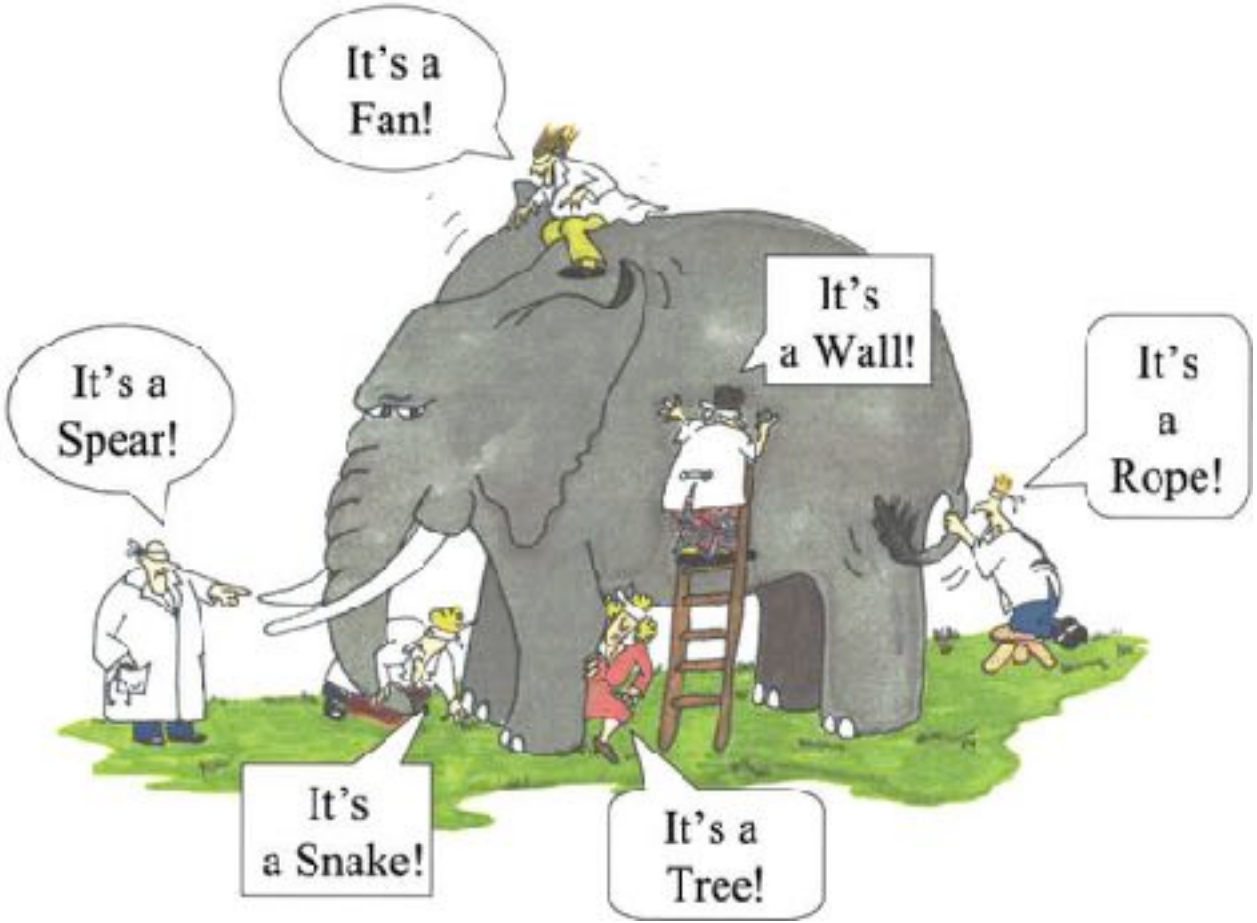
It's a Fan!
It's a Spear!
It's a Wall!
It's a Rope!
It's a Snake!
It's a Tree!

citynetwork

Security

≠

Compliance

citynetwork

Compliance is about surviving audits

Audits is about surviving checklists

citynetwork

‘**personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘**processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘**personal data breach**’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Privacy by Design

citynetwork

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organizational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:

CAUTION

citynetwork

- ✓ Follow best practice guides
- ✓ Ensure your software is vulnerability managed
- ✓ Have a Security Incident Response Team
- ✓ Ensure you can track full accountability on your infrastructure
- ✓ Don’t forget cross connect rooms for LAN

citynetwork

If you know the severity is high and do not follow best practice

=

Hard Sell!

Accountability

=

Monitoring, Logging and Reporting

Nothing decreases risk as much as human hands off

Automate

Ansible, Puppet, Chef, Salt

NFV is your friend

Everything you can define as a service is your friend

citynetwork

Continuous security configuration

Continuous security hardening

Continuous access controls

Continuous log rotation

citynetwork

DevOps

=

SecOps

- ✓ Report incidents to authorities
- ✓ Security organization
- ✓ Security response team
- ✓ Security escalation channels
- ✓ Continuous improvement
- ✓ Code review
- ✓ Regular penetration testing
- ✓ Best practice guides

citynetwork

Keep logs

Analyze logs

Secure logs

Monitor Security events

- Successful authentications
- Unsuccessful authentications
- Audits being run
- Audits failed to run
- Changes in firewalls

Control your PKI

citynetwork

Everything which is not forbidden is allowed

Golden rule of policy configuration:

everything which is not allowed is forbidden

http://docs.openstack.org/mitaka/config-reference/compute/policy.json.html

citynetwork

allow from <target> to <destination> port <port number> proto <protocol name>

No ranges only specific hosts

Deny all is default on both inbound and outbound traffic

citynetwork

Follow PCI-DSS
or
ISO27018

citynetwork

Thank you!

@Hindart
kim.hindart@citynetwork.se

citynetwork