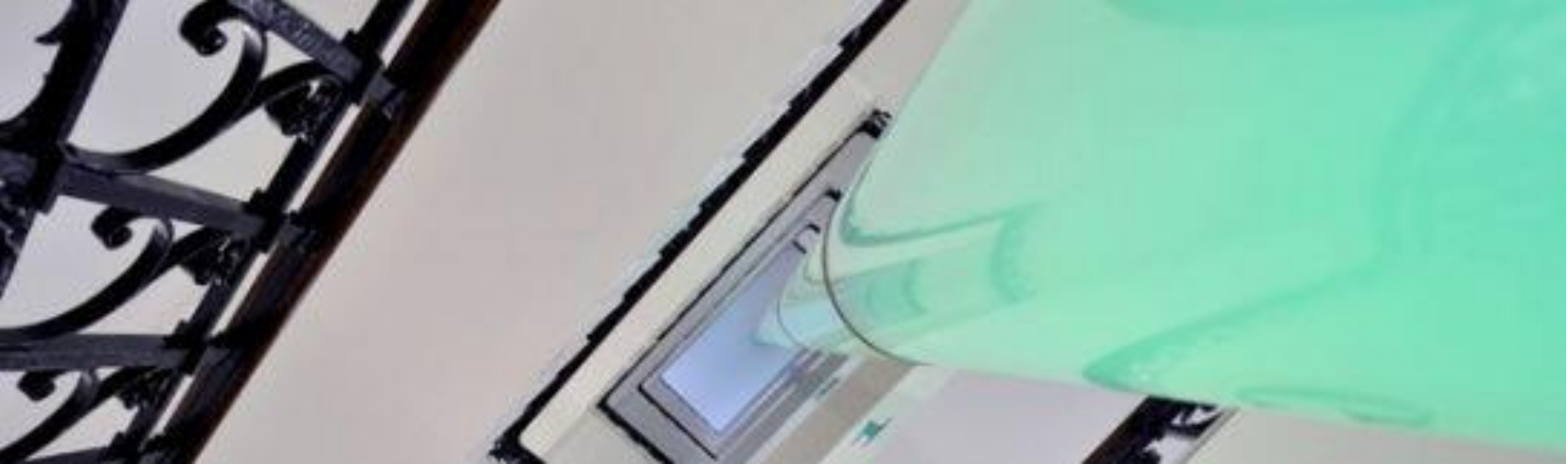


Trust Boundaries In the Cloud

CLOUDSEC UK 2016

Marc Lueck

Company85
accomplish more™

Cloud Has Arrived

95% of Businesses Using Cloud

1083 Cloud Services PER ENTERPRISE

Just 7% meet our Security Requirements

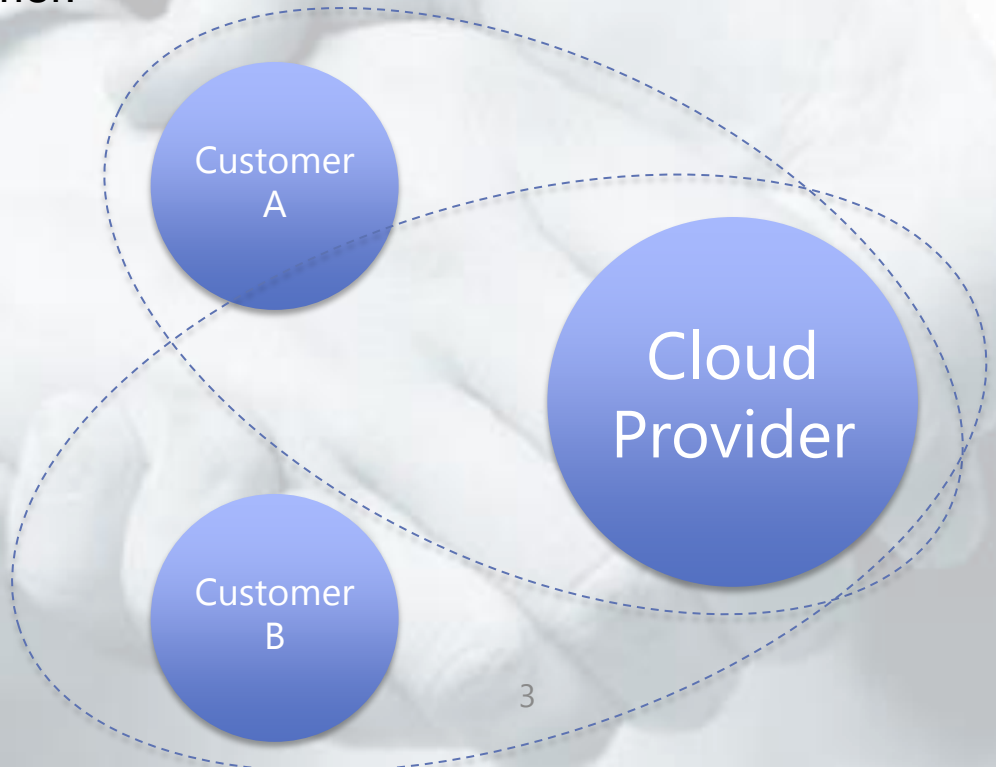
Security no longer #1 Challenge

We have extended our trust boundary – and begun to trust cloud providers implicitly

What is a Trust Boundary?

Trust Boundary [truhst **boun**-d*uh*-ree, -dree]

A logical perimeter that typically spans beyond physical boundaries to represent the extent to which IT resources are trusted. When analysing cloud environments, the trust boundary is most frequently associated with the trust issued by the organisation acting as the cloud consumer.



Implicit Trust

Explicit Trust

Trust Boundary Impacts

Internal/Our Own

- Visibility of all data from security tools
- Know everyone with access to your data
- Understand compliance against your corporate standards.
- *Rarely perfect but you know which cupboards the skeletons are in.*

Cloud Provider

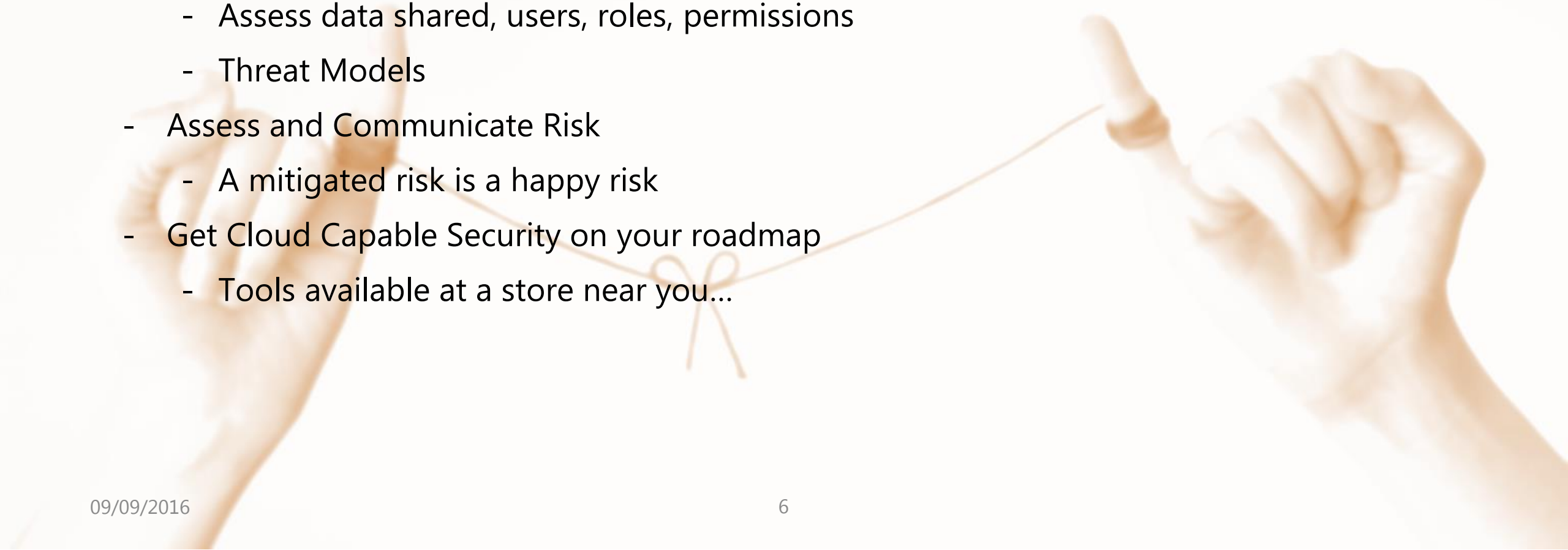
- Lack of Transparency
  - Typically limited visibility of data from security tools – you are trusting they are being monitored/actioned
  - Compliance, where available, is only as reliable as its scope – and this may not be visible to you
- Loss of control – often little or no control or knowledge over access to your data
- Low/no influence on processes and tools that are implemented.
- *Security may be better than your own, but how do you know?*

Implicit Trust – dangerous practices

- Extending the trust boundary while maintaining liability. Increasing cloud provider's liability will undoubtedly increase the cost.
- Trust normally inversely proportional to the business
  - IAAS PAAS SAAS
  - Lowest <-> Highest
- Limited visibility
- Multi-Tenancy – where IS my trust boundary exactly?
- Custom/add-on security is expensive – reducing benefits of cloud
- Incident Management – SLA minefield

Moving from Implicit Trust – Trust but Verify

- Document, document, document! Visibility is key.
  - Assess data shared, users, roles, permissions
  - Threat Models
- Assess and Communicate Risk
  - A mitigated risk is a happy risk
- Get Cloud Capable Security on your roadmap
  - Tools available at a store near you…



Cloud Security doesn't mean Delegated Security

- Your internal security team is still absolutely essential
  - Add Cloud to your SOC/Security team responsibilities
  - Assess and review - just what security data IS provided by cloud provider?
  - Include cloud security in your reporting – including gaps!
- Build out and test Incident Management
  - What if your breach involves a cloud provider?
  - Have you aligned SLAs and internal IM?
  - Ensure incident management is risk based – back to your documentation

When all else fails…

- Encrypt if you can
- Get it in the contract
- Insure against the worst

Thank you – any questions?

Marc Lueck, CISO

Company85

www.company85.com