Cogito Group
DIGITAL IDENTITY AND SECURITY

cogitogroup.com.au

The changing face of cyber security

Presented by Richard Brown

Historically…

Traditional data protection: the castle defence strategy

- Strong protection of the border involved:
  - Restricted entry based on entry points (ports)
  - Then came SPI, DLP etc
- On compromise only options were:
  - Further restrict entry points
  - Restrict access methods (eg VPN)
  - Still have a host of vulnerabilities.
- These are still all relevant, but…

Today…

Rapidly changing landscape

- We need ever more flexible access
- Threats often don't use the front door
  - The trusted insider threat
  - Bring Your Own Device
  - Systems are no longer just on premises but in the cloud too
  - More of the enterprise is accessible via the internet.
  - Access is by not just employees, but now also contractors, customers and partners
  - Accessed any time from anywhere in the world
- Once your inside the network most organisations have very few restrictions.

The challenge

Usability versus security

- Business now expects high levels of connectivity between applications, devices and individuals.
- Security must adapt to this.
- Security needs to:
  - See past one box or solution.
  - A layered approach gives greater assurance
  - Authentication and encryption are essential components.
  - Adapt to internet scale rather than enterprise scale.
  - The boundary is still important

The internet of threats

- Gartner prediction of 25 billion connected things by 2020
- Need to make them more useful
  - Better relationships: Individual to individual, individual to device and device to device.
  - Delegation with accountability (eg UMA)
  - Improved security through
    - Contextually aware dynamic decision making
    - Improvement of Behavioral analytics
  - Sharing while maintaining control
  - More automation but still need the ability to have approval workflow and handle exceptions.

The future


YESTERDAY
"Isolation"
TODAY
"Building Bridges"
TOMORROW
"Total inter-connectivity"
ID Card

The New Look Castle

Next Generation Firewalls

- Boundary Protection still plays a role
- New and improved guards at the entrance:
  - Heuristic techniques
  - Content identification
  - Rules based on user identification
  - Decryption and inspection of secure packets
  - Filtering and checking based on daily updates (eg URL and AV)

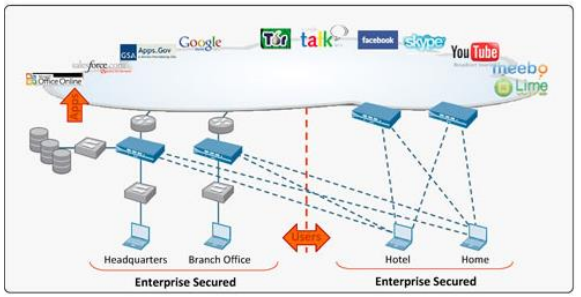


*Image courtesy of Palo Alto Networks

Identity is KEY

- An ‘entity’ may be:
  - a person
  - a device
  - a third party
  - Entities include users from outside the organisation and may represent a group or role.
- Organisations now need to gain an understanding of the relationships it has with identities.
- You need to get it right from the start and to the end
- Provisioning, update and de-provisioning are key

Access Control

- Seamless access to users to authorised systems
- Know who and what is accessing your data
- Provisioning rules
- Allow automated and supervisor approvals of special access

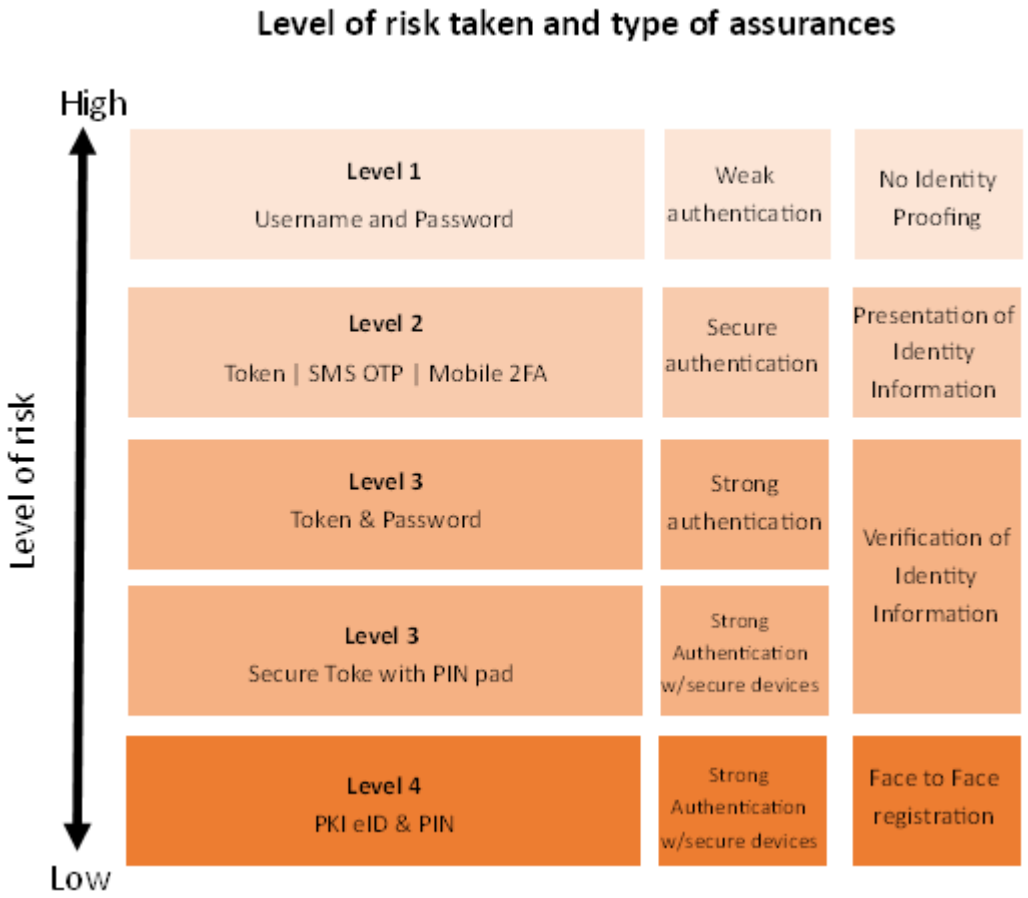
Authentication

- Go beyond passwords to:
  - Ensure better level of authentication
  - Hackers can’t access data once past firewall
- Systems authenticate (not just users):
  - Share data ONLY with other known and trusted systems
  - Not with a hacker or foreign system

Multi Factor Authentication

- One of the most effective measures to prevent a cyber-intruder
- MFA is the provision of multiple pieces of information
- Enables tasks such as system authentication.
- Edward Snowden proves why this can be so effective.

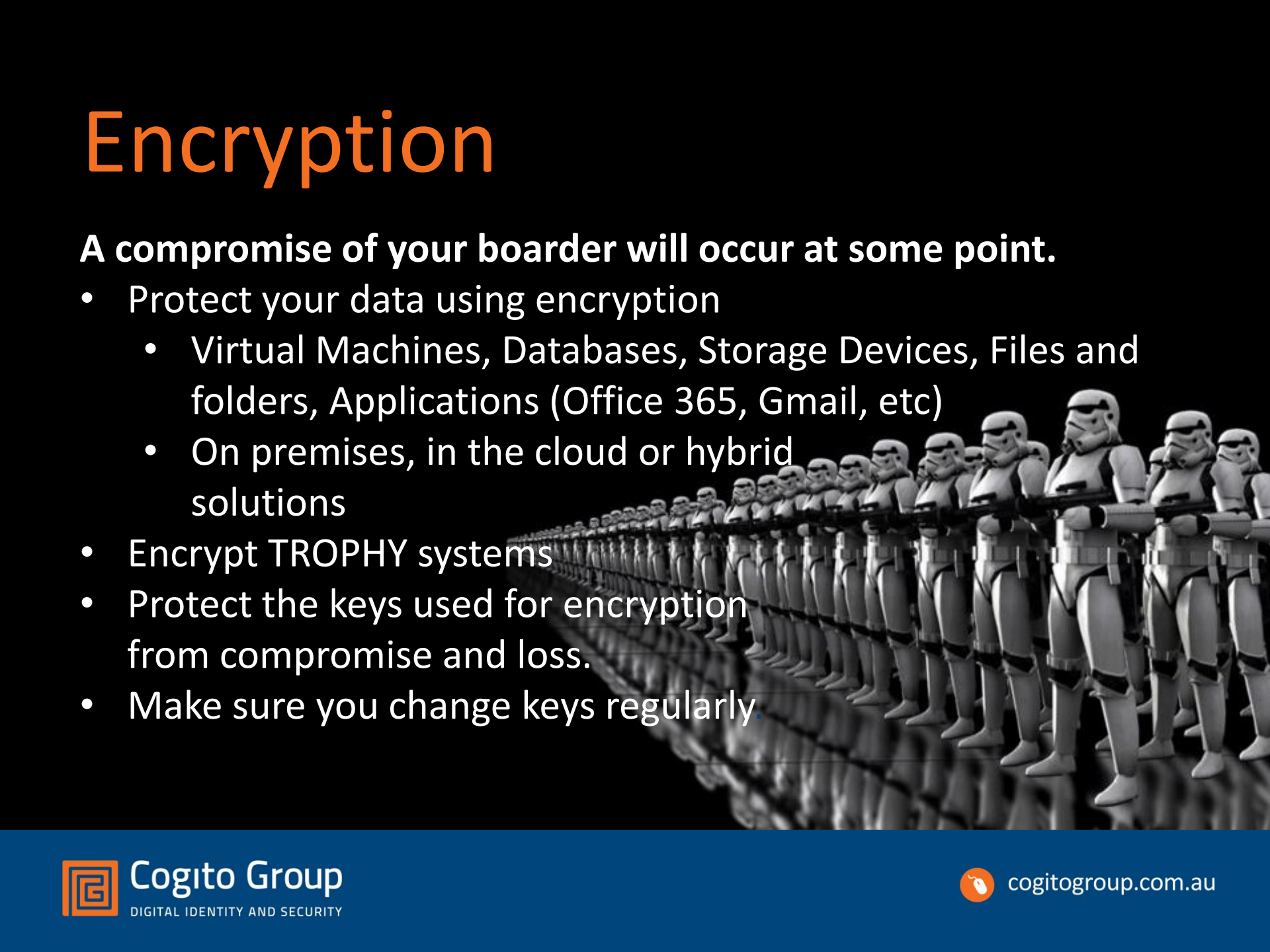
Levels of Assurance



Encryption

A compromise of your boarder will occur at some point.

- Protect your data using encryption
  - Virtual Machines, Databases, Storage Devices, Files and folders, Applications (Office 365, Gmail, etc)
  - On premises, in the cloud or hybrid solutions
- Encrypt TROPHY systems
- Protect the keys used for encryption from compromise and loss.
- Make sure you change keys regularly.



Keys

- Keys to the kingdom stay in control of the castle owner
- This is true for data kept:
  - On-premise
  - Cloud
  - Hybrid
- Keeping the keys still means:
  - The trusted cloud service providers host the data, but have no access to the information.
  - On-premises administrators don't need to see the data to perform their roles
  - Castle owner decides who has access to the informaiton

Thank You

Thanks for listening.

Please direct any further questions to:

Richard Brown
CEO, Cogito Group

sales@cogitogroup.com.au

www.cogitogroup.com.au
cogitogroup
Cogito Group Pty Ltd
@CogitoGroup1