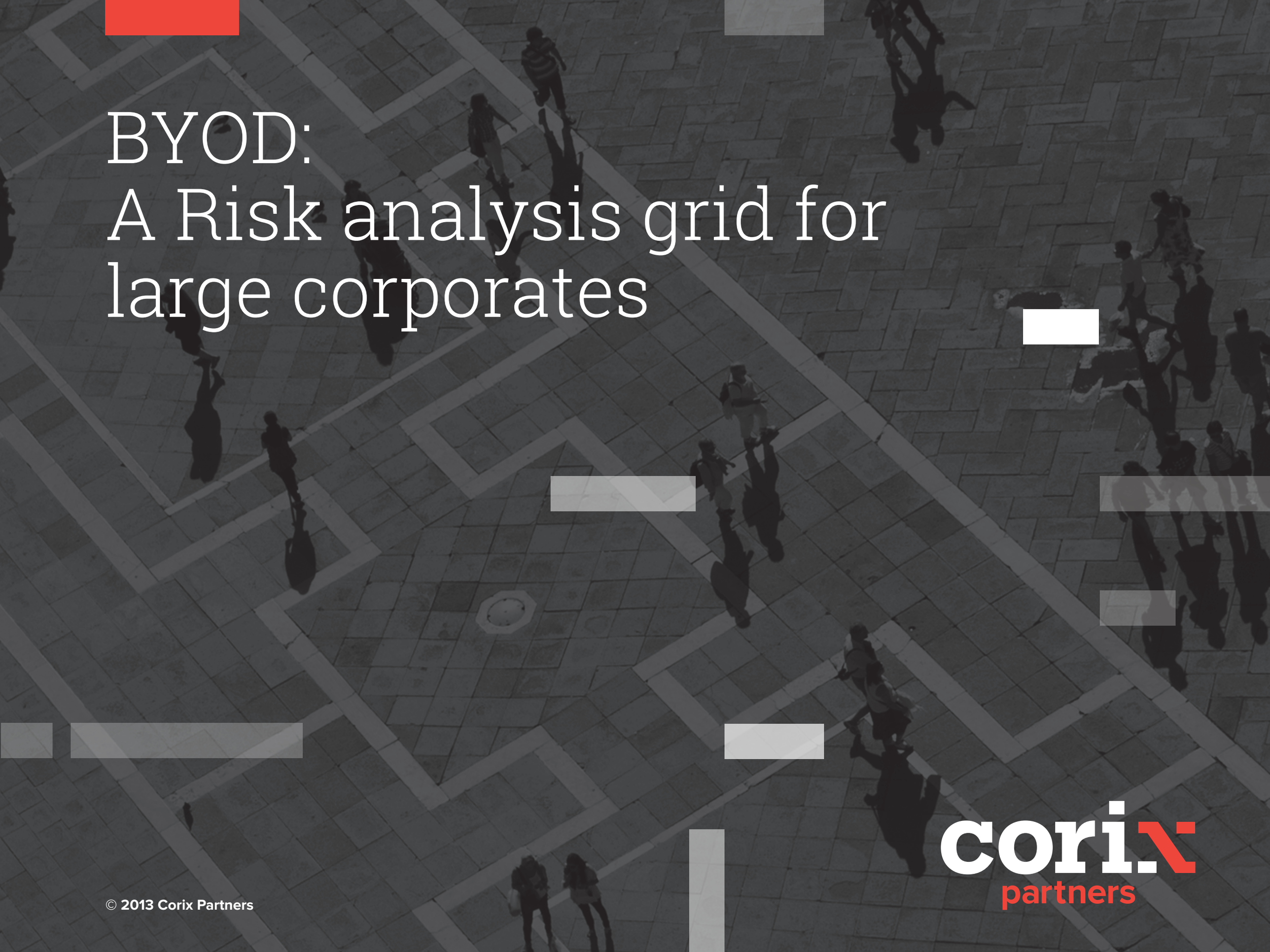
BYOD:
A Risk analysis grid for large corporates



corix
partners

BYOD: A complex topic for large corporates

- **A large proportion of staff bring personal devices to the office everyday, and use them through public networks**
  - – A greater diversity of data-enabled devices, applications and Cloud services available to the general public, increasingly more innovative, affordable and powerful
- **Should staff be allowed to use these personal devices in the regular performance of their work duties?**
  - – Where? When? To do what?
- **Does this offer opportunities to large corporates?**
  - – To achieve what? And at what Risk?
  - – In a context where all have very large IT investments, legacy and staff base
  - – And most are cutting costs significantly through the current economic downturn

BYOD: One same acroynm and a lot of hype, hiding a variety of situations

Bring Your Own Device. Where? When? And to do What?

BYOD everyday to the office and use it to work instead of using acorporate desktop / laptop?

BYOD with you when travelling for work instead of using a corporate laptop/ mobile phone/PDA/ Blackberry?

BYOD to the office for personal use and expect to connect it to some corporate network?

BYOD where ever you go and and use it to access corporate email (only)

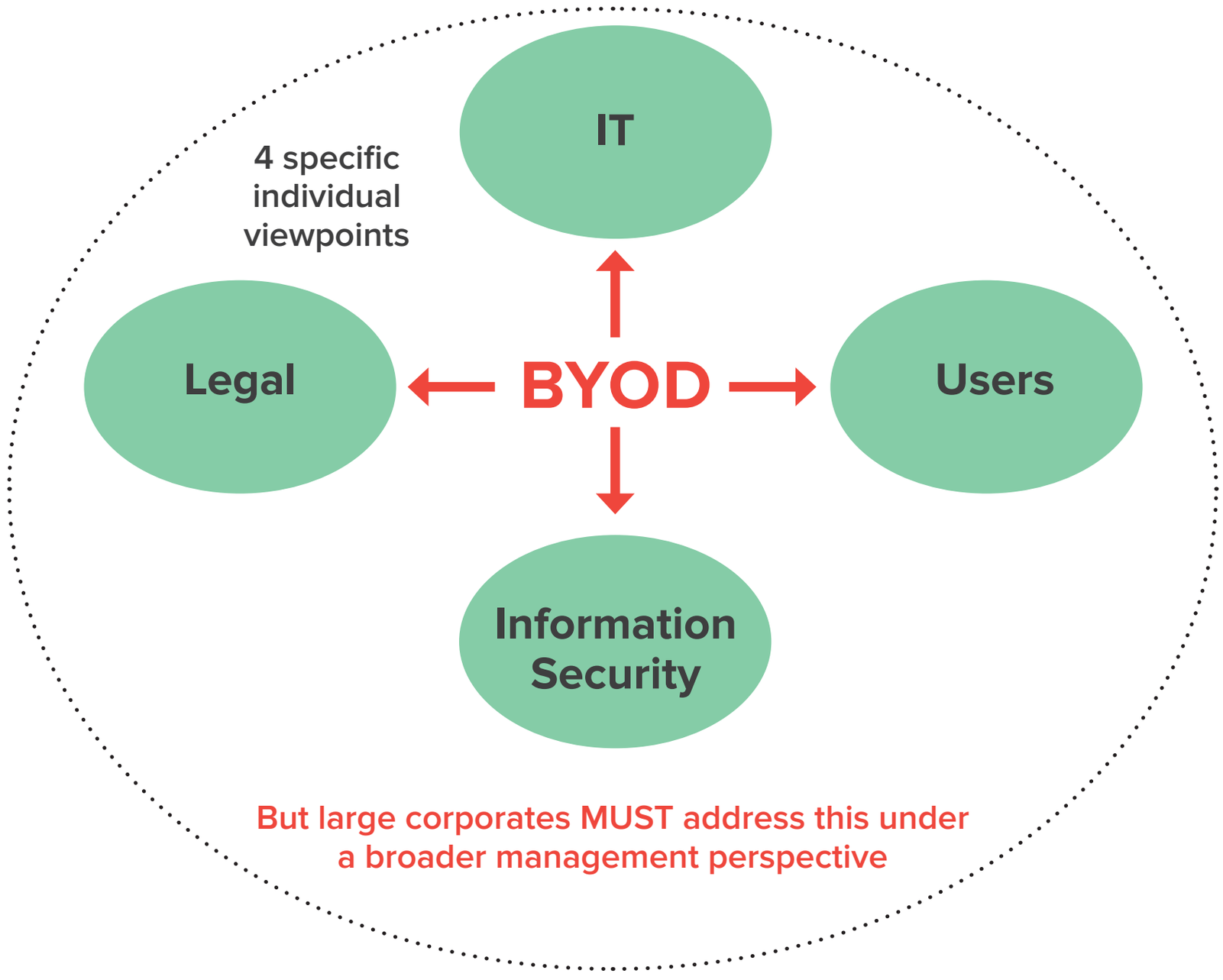
What corporate device is being replaced by a personal one?

– The corporate desktop?
– The corporate laptop?
– The corporate mobile phone/PDA/Blackberry?
– All of the above? None? A combination?

On what scale?

– Allowing vs. Mandating

BYOD: A number of different angles to consider



But large corporates MUST address this under a broader management perspective

BYOD: The view from the IT Department

- **Large scale BYOD schemes offer potential opportunities to cut costs, in a context of high budgetary tensions**
  - – By avoiding a hardware refresh where desktop and laptop estates are reaching end-of-life, and cutting on associated deployment and ongoing support costs
  - – By cutting on mobile phone contracts, where those are due for renewal
  - – By cutting on expensive and complex licenses management programmes
- **An off-load of significant support responsibilities onto user populations**

BUT DON'T OVER-SIMPLIFY

Who really pays for what in a large BYOD scheme? (hardware? software? roaming charges?)

Can the staff assume support responsibilities professionally and sustainably over time?

(Can you force it upon them? And who does what when the device stops working/is lost/stolen?)

BYOD: The view from (some) user populations

The latest technology as a status symbol

Bypassing IT corporate refresh cycles that cannot keep up with those on the consumer market

And are perceived as archaic by some younger user populations that are increasingly more technology aware
and are used to having the latest technology

But how widespread is this culture across the company?

A greater level of control over the everyday work device

Bypassing corporate support processes that are structured around complex (legacy) IT environments and large populations of users

And perceived as slow and bureaucratic by some younger user populations that are increasingly used to having some form of self-maintaining free technology

But are support levels that bad?

Better support for flexible working practises device

The multiplication of portable electronic devices (and their chargers, cables, adapters etc ...) is unpractical for a workforce that is increasingly adopting flexible working practices

BYOD brings an opportunity to reduce that complexity

But is this based on a real business need or just convenience?

BUT DON'T GET CAUGHT INTO A SIMPLISTIC GENERATION GAME:

Look beyond social trends, technology fashions and gadgets: Can BYOD increase staff performance?

What is the real culture that the company wants to build around technology and mobility?

BYOD: The view from Information Security

This is nothing REALLY new

Staff have been using their own devices for years, typically to work from home from time to time

Where relevant, Data Leakage Prevention (DLP) products may already be in place (typically to control what is taken home on USB devices etc…)

All should already be covered in Information Security policies and education programmes

What changes is the scale

BYOD turns an occasional productivity arrangement allowed by exception, into a permanent working practice

And boundaries disappear between personal and professional usage of the same device (a device that may even be shared)

Information leakage risks increase exponentially

All pre-existing Security arrangements need hardening

Including policies, education programmes, and the settings of DLP products (where in place)

Good segregation and sand-boxing principles apply and must be enforced, together with some form of usage monitoring practice

Insufficient or weak Security practices must be uplifted

BUT DON'T BE COMPLACENT:

What is the real Security maturity of the company around these matters?

Is the company ready for the security challenges a large scale BYOD scheme may bring?

BYOD: The view from the Legal Department

The company has an overall duty of care over Information

and may be found negligent if it fails in that duty of care

The company needs to maintain adequate records and the ability to investigate Information breaches

How do you handle serious incidents, if the work device cannot be examined because it is not owned by the company?

How do you frame and manage liabilities?

In a context where the work device is no longer owned by the company

Who is liable if illegal (unlicensed) software is used by staff to deliver work on behalf of the company?

Who is liable against the terms of Cloud services, if those are entered into by staff to deliver or support work on behalf of the company?

How do you work with unknown terms and varying jurisdictions?

In a context where they are directly entered into by staff to deliver work on behalf of the company

In a context where they may contradict some obligations of the company towards its clients

In a context where staff and their work devices may be travelling on a global scale without consideration of the Information they carry.

A POTENTIAL LEGAL MINEFIELD

If you allow BYOD practices to creep in through the back door uncontrolled and on a large scale

BYOD: The view from Management

- **Can BYOD make the company work better?**

  – By increasing staff motivation and performance, and making the company more agile
  – By making the company more attractive to younger workers
  – WHILE driving IT costs down
  – WITHOUT introducing additional / unwanted / unmanaged risks

- **Is this a long-term irreversible social trend, or another IT cycle?**

- **Are there real business needs behind all this, or is it just convenience?**

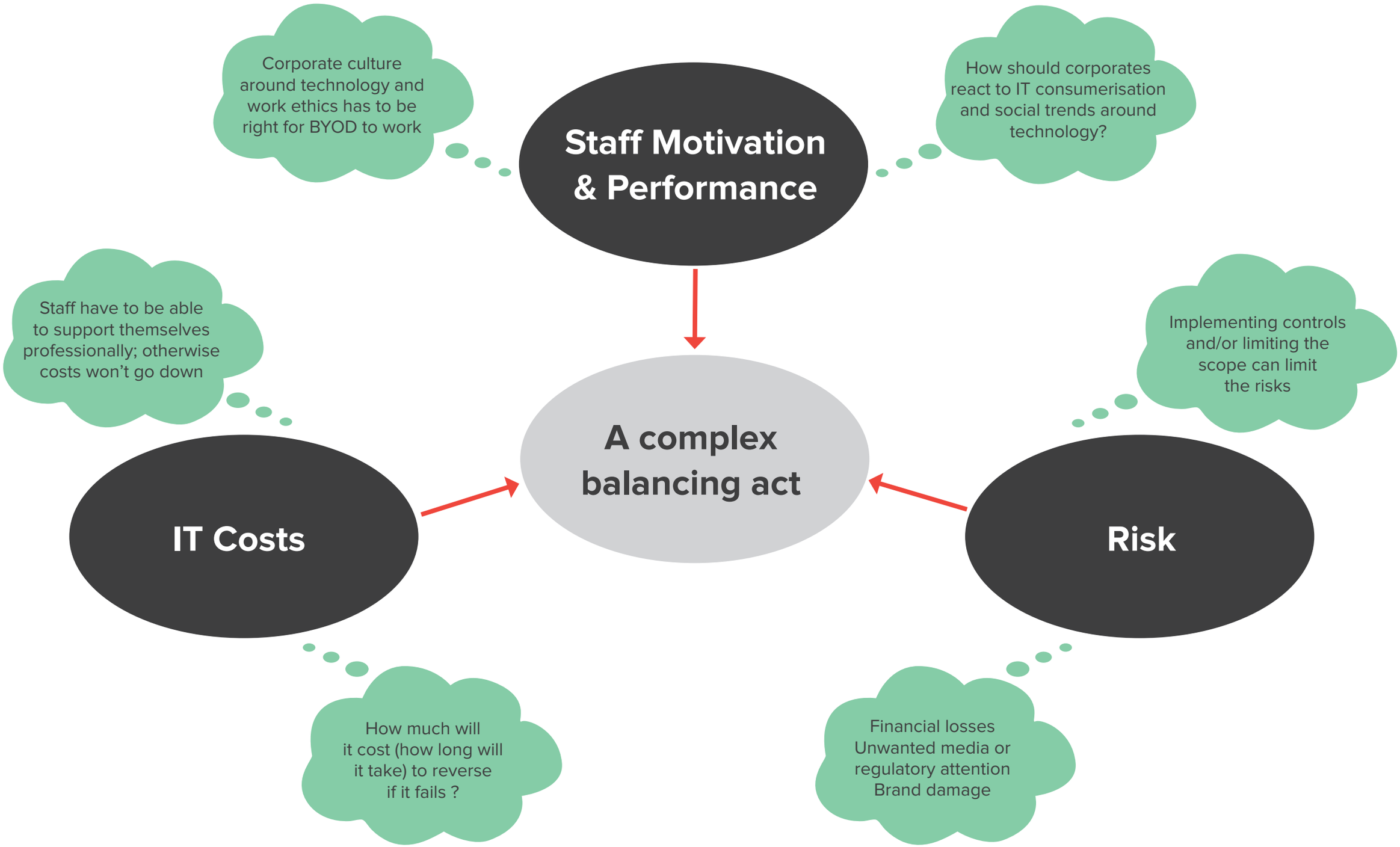
- **How much will it cost (how long will it take) to reverse if it does not work?**

A COMPLEX BALANCING ACT, in a context where:

The work device (corporate or privately owned) has to remain a stable productivity platform

The work device (corporate or privately owned) has to remain a secure and lawful platform

BYOD: The Management balancing act



BYOD: Key aspects to consider and Risk mapping

BYOD: Key Recommendations

- **This is not just an IT matter: Make the decision in consultation with all parties**

- **This is not for everyone: Only get into it where it fits your corporate culture**
  - Right scale / right staff / right training: DO NOT FORCE IT ON PEOPLE
  - When determining the scope, ALWAYS consider the sensitivity of each role and the information people have access to

- **Harden the business case: Factor Security and training costs at the right level**
  - Implement Security sandboxing as much as realistically possible, and strengthen Data Leakage Prevention arrangements
  - Base your training estimates on the real IT maturity of the staff and don't assume everybody knows about computers

- **Frame it with a strong policy: Be clear and specific from the start on:**
  - The Information Security obligations of the staff, and the level of monitoring that will be taking place
  - The legal and licensing obligations of the staff
  - Support arrangements and demarcation lines with the corporate IT department
  - Who pays for what, on day 1 and beyond about computers

Contact

For further information please contact:

Jean-Christophe Gaillard
Managing Director
+44 (0)7733 001 530
jcgaillard@corixpartners.com

Neil Cordell
Director
+44 (0)7701 015 275
neilcordell@corixpartners.com

www.corixpartners.com