What is the right level of maturity for your organisation?

Stephen Bailey, Associate Director

What is the ***right*** level of maturity for your organisation and ***how*** do you get there?

Why ask?

86% Say their cyber security function does not fully meet their organisation's needs

69% Of responders say they need up to 50% more budget

62% Would not increase their cyber security spending after experiencing a breach which did not appear to do any harm

*EY 2016 Global Survey

Issues?

Poor planning and articulation of the issue at Board level often leads to:

Gold standard over investment

Under investment

No investment or ignorance

Major incident/breach

*EY 2016 Global Survey

What happens next?


“Get me an independent review”


“Tell me what the gaps are!”


“Where do we really need to be?”


“How will we know when we have done enough?”

What happens next?

Simple as that

Initiate, define and evaluate

Context

ISO 27001

NIST

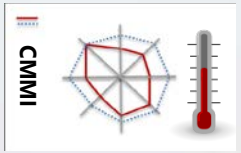
COBIT

GDPR

Others

Control Domain Assessment

Current State
AS-IS



Future State
TO-BE

INITIATE
DEFINE &
EVALUATE

Build the plan for success

Brilliant. Fix it. I want to be there! Tomorrow!

Deliver effective change?

Where is this stuff?
Why can’t I see anything yet?
I’m not doing that!
You’re inhibiting my growth!

Reality hits!

Takes too long to see results

Board loses interest

Not enough resources

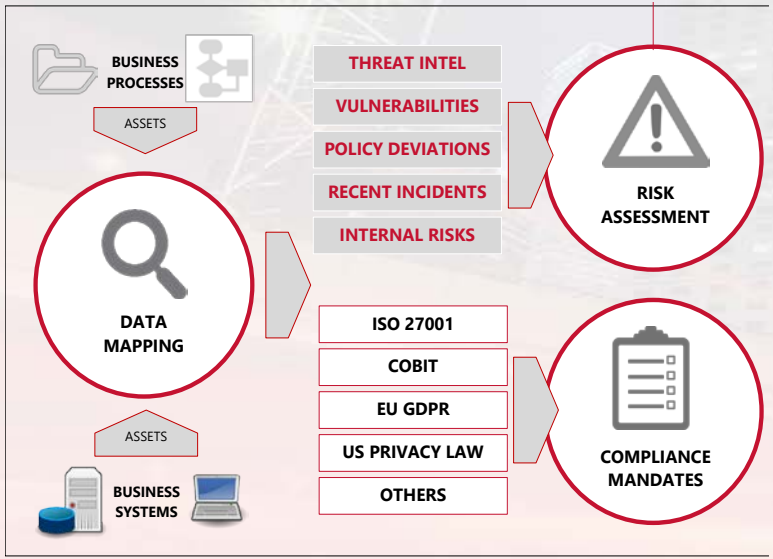
Stakeholders lose interest

Stop the programme!

What went wrong?

1. A maturity review is much more than a control assessment
2. Improvements were planned as a project, not a transformation programme
3. Other transformation initiatives were not factored in

Improvements

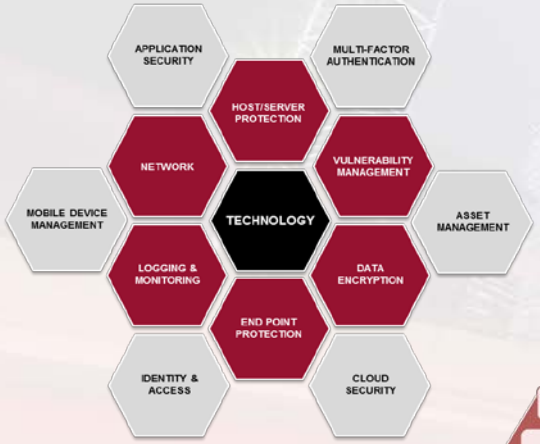


Assessing the right level of Maturity is more than just a review against control domains

- Include a threat/risk assessment
- Cover process and systems reviews
- Build it on a good understanding of your assets – i.e data mapping

…..as a start

Improvements – Planning



- People, process, technology
- ISMS, tech control improvements
- Target operating model, organisation, skills, resources, responsibilities
- Good project management
- Look at the holistic operating model and dependencies

…..as a start

So how can it be done better?

If it is a real transformation it needs to be treated with the same commitment and approach as any other major transformation programme

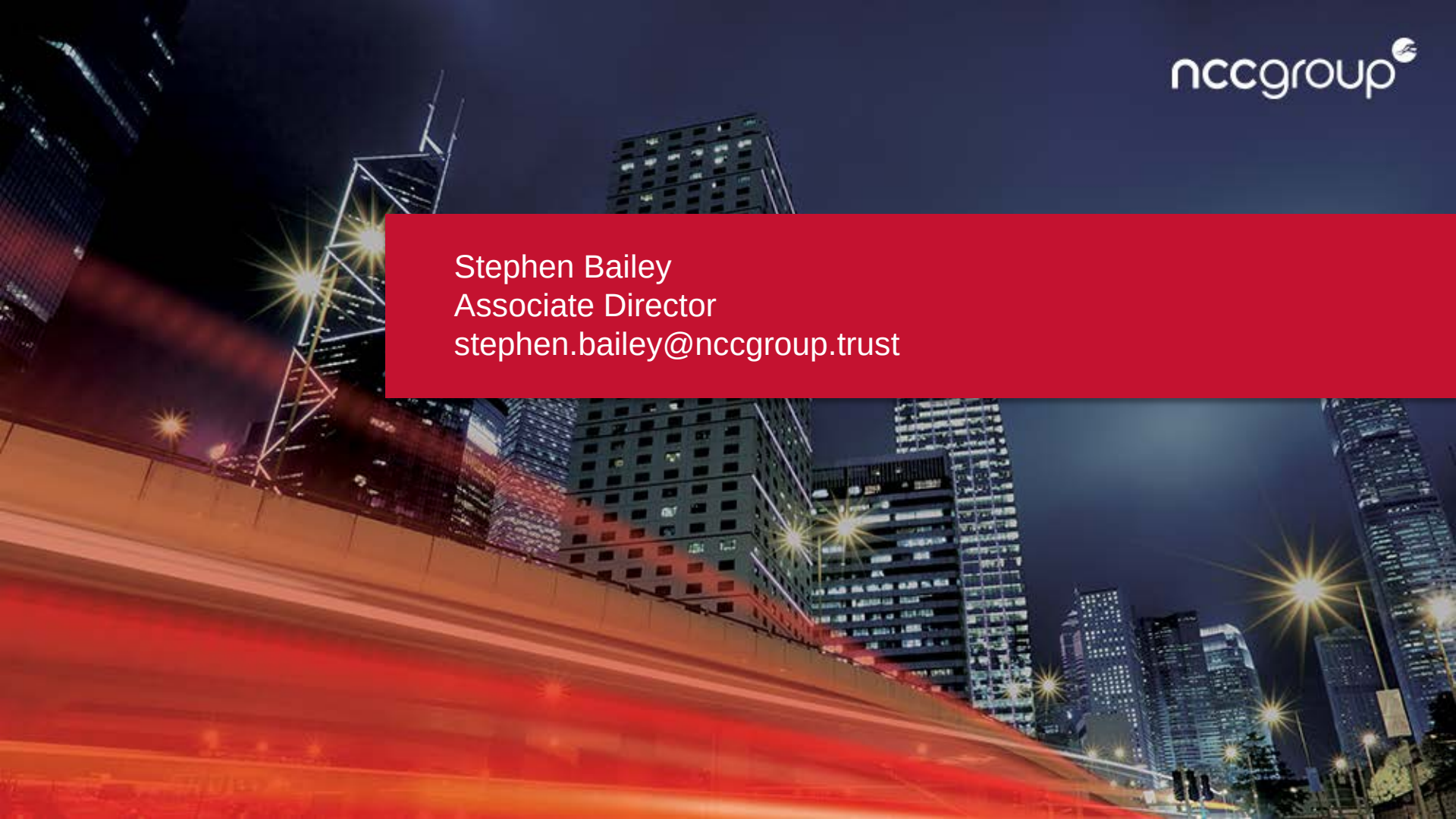
Reality – treat it like real transformation

- ***Change*** – Well defined initiatives, usually impacting one part of the organisation. Usually executing a well defined shift in the way things work.
- ***Transformation*** – Usually a portfolio of initiatives with dependencies and could end up with a new business model and vision for the future

- Key stakeholder buy in
- Obtain effective leadership experienced in transformation not just Information Security
- Get the target level right
- Organisations can only undergo a certain amount of change in any period
- Understand the readiness for change

Simple success factors

- ✓ Board influence and buy-in
- ✓ Effective CISO/Leadership
- ✓ Strong and effective team
- ✓ Right methodology
- ✓ Know what you are competing with
- ✓ Know what you are complimentary to
- ✓ Maintain board presence
- ✓ Keep communicating
- ✓ Demonstrate risk reduction
- ✓ Demonstrate legislative compliance (if applicable)
- ✓ Show improvements to the business (e.g. faster time to market)
- ✓ Right metrics/dashboard



Stephen Bailey
Associate Director
stephen.bailey@nccgroup.trust