# NOTHING TO SEE HERE!

# A PowerPoint Slide Presentation

By Andrew Kelly

# Abstract: OWASP Day 2013

This is how it starts: **"Seeking an exciting new challenge...?"**

- Is there, in fact, any such thing as a greenfield security opportunity left in the wild? And ... if such mythical beasties do exist ... are they worth signing on for?
- The pros and the cons of setting up of an information security function in an organisation from scratch ('Greenfield'); as opposed to trying to bed yourself down into an already-existing organisation ('Brownfield').

*So ... if you want to hear a guy speak who reckons he's forgotten more than he ever thought he knew? Then this is so the talk for you!*

# All About Me

**Health Benefits Ltd.**, Auckland, NZ [2013 on]; **Telecom Ltd.**, Auckland, NZ [2012-2013]; **Lateral Security (IT) Services Ltd.**, Auckland, NZ [2010-2012]; **Security-Assessment.com Ltd.**, Auckland, NZ [2007-2009]; **Transpower Ltd.**, Wellington, NZ [2006-2007]; **BT Syntegra Ltd.**, London, UK [2006]; **Fonterra Co-operative Group Ltd.**, Auckland, NZ [2004-2005]; **BT Syntegra Ltd.**, Leeds, UK [2004]; **Insight Consulting Ltd.**, Walton-on-Thames, UK [2003]; **National Bank of NZ Ltd.**, Wellington, NZ [2003-2004]; **Royal Bank of Scotland Group**, Edinburgh, UK [2002]; **Halifax/Bank of Scotland**, Leeds, UK [2001]; **Banque Nationale de Belgique**, Brussels, Belgium [2001]; **Deutsche Bank Ltd.**, London, UK [2000-2001]; **Lloyds/TSB Bank Ltd.**, Southend-on-Sea & London, UK [2000]; **Bank One International/First USA Bank**, Cardiff, UK [1999]; **Générale de Banque**, Brussels, Belgium [1998-1999]; **Perot Systems Europe Ltd.**, Nottingham, UK [1997-1998]; **Chartered Trust Plc (Standard Chartered Bank)**, Cardiff, UK [1996-1997]; **Legal & General Assurance**, Kingswood, Surrey, UK [1996]; **Sun Life Assurance Company of Canada (UK) Ltd.**, Basingstoke, UK [1989-1993]; **Databank Systems Ltd.**, Wellington, NZ [1988-1989]

# 25 Years…

July 1988: ‘Promoted’ to Data Security Officer, Databank Systems Ltd., Vivian Street Data Centre, Wellington.

People have accused me of being bitter, twisted, cynical and a complainer!

Me!

I know, right!

# 25 Years…

July 1988: ‘Promoted’ to Data Security Officer, Databank Systems Ltd., Vivian Street Data Centre, Wellington.

People have accused me of being bitter, twisted, cynical and a complainer!

Me!

I know, right!

I am ***not*** ‘twisted’…

# “You’ve Got Mail…”

*“Seeking an exciting new challenge? Want to be responsible for building and shaping an embryonic information security function? Then you so won't want to miss this golden opportunity!”*

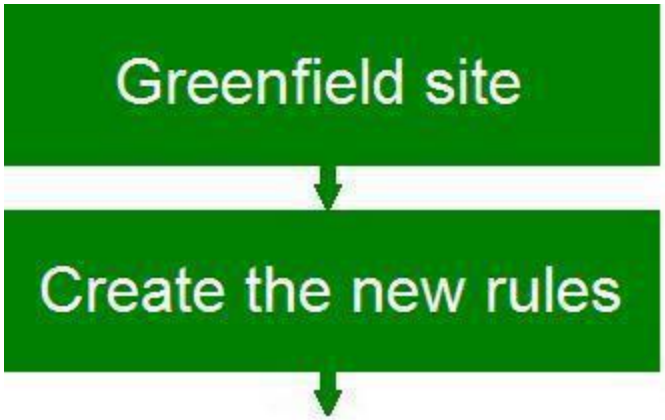
# GREENFIELD VS. BROWNFIELD

Greenfield

Brownfield

# Greenfield vs. Brownfield

# Greenfield vs. Brownfield



# Greenfield vs. Brownfield

"Create the new rules":

*"The term greenfield was originally used in construction and development to reference land that has never been used (e.g. green or new), where there was no need to demolish or rebuild any existing structures.*

*Today, the term greenfield project is used in many industries, including software development, where it means to start a project without the need to consider any prior work."*

Webopedia

# Greenfield vs. Brownfield

# Greenfield vs. Brownfield

# Greenfield vs. Brownfield

"Change the old rules":

*"The term brownfield was originally used in construction and development to reference land that at some point was occupied by a permanent structure.*

*In a brownfield project the structure would need to be demolished or renovated.*

*Today, the term brownfield project is used in many industries, including software development, to mean to start a project based on prior work or to rebuild (engineer) a product from an existing one."*

Webopedia

# Greenfield vs. Brownfield

# Greenfield vs. Brownfield

“Transformational change”, my definition:

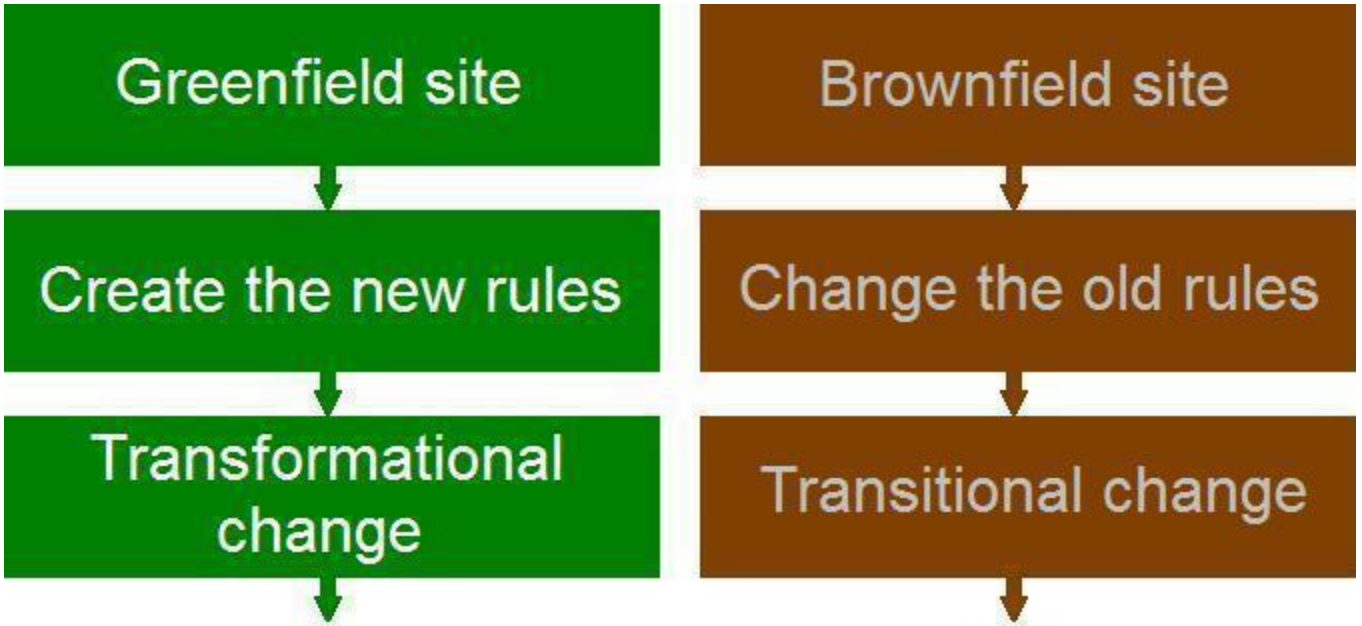
‘Greenfield’ doesn't necessarily mean a new startup.

It could mean an organisation where (~~information security has been ignored up until now~~) a distinct information security function hasn’t been set up as yet.

For example: Prior to the appointment of a CISO, CSO, Security Manager, Security Analyst, etc.

Or it can mean a new startup...

# Greenfield vs. Brownfield



# Greenfield vs. Brownfield

“Transitional change”, my definition:

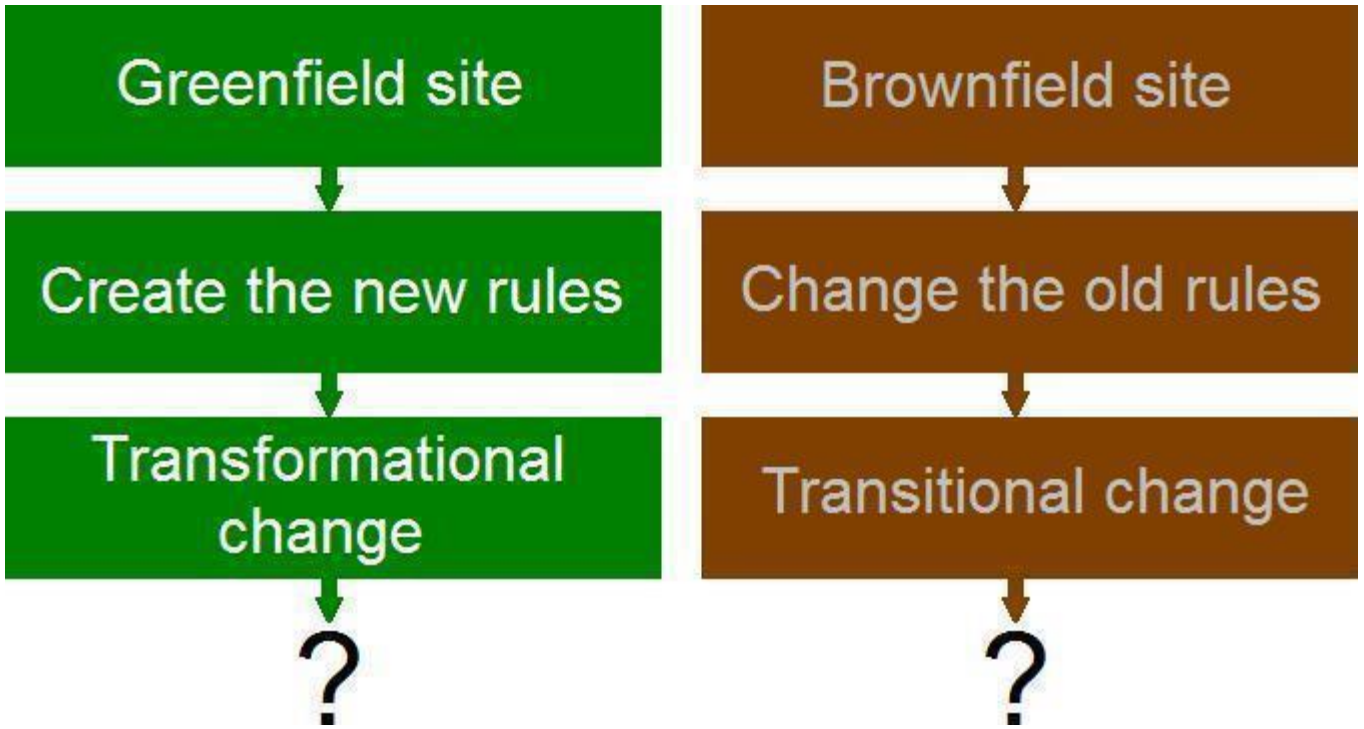
‘Brownfield’ doesn't necessarily mean the previous incumbent rage-quit.

It could mean an organisation where (~~information security has been done all wrong up until now~~) a newly appointed information security function has a chance to build on what’s already been achieved.

For example: You’ve just been appointed as the new CISO, CSO, Security Manager, Security Analyst, etc.

Or it can mean the previous incumbent rage-quit...

# Greenfield vs. Brownfield



# ARE GREENFIELD'S MYTHICAL?

**Question:** *"Is there any such thing as a greenfield security opportunity left in the wild?"*

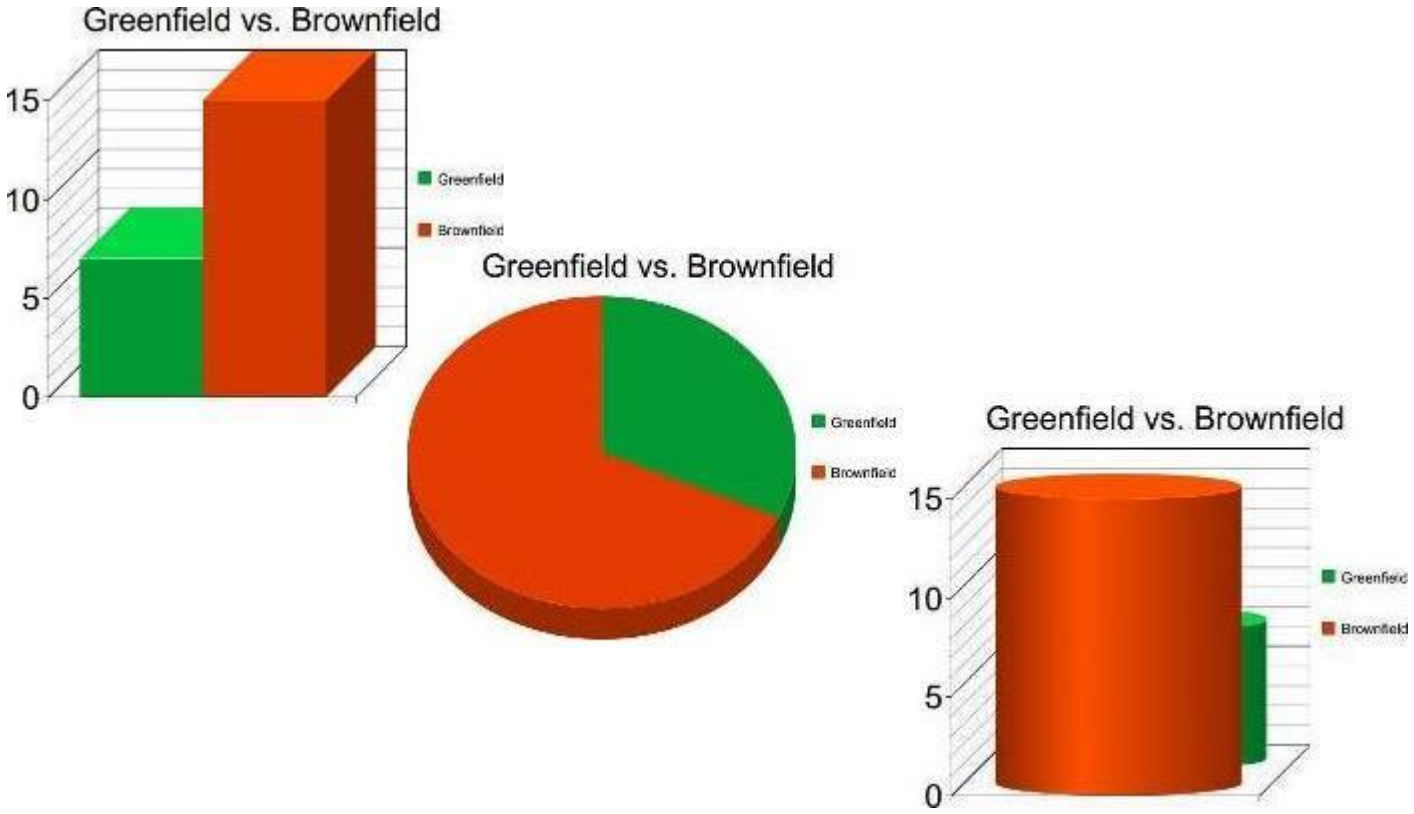

There's a caveat: When talking 'startup', I'm talking a non-security focused business here.

# Are Greenfield's Mythical?

**Health Benefits Ltd.**, Auckland, NZ [2013 on]; **Telecom Ltd.**, Auckland, NZ [2012-2013]; **Lateral Security (IT) Services Ltd.**, Auckland, NZ [2010-2012]; **Security-Assessment.com Ltd.**, Auckland, NZ [2007-2009]; **Transpower Ltd.**, Wellington, NZ [2006-2007]; **BT Syntegra Ltd.**, London, UK [2006]; **Fonterra Co-operative Group Ltd.**, Auckland, NZ [2004-2005]; **BT Syntegra Ltd.**, Leeds, UK [2004]; **Insight Consulting Ltd.**, Walton-on-Thames, UK [2003]; **National Bank of NZ Ltd.**, Wellington, NZ [2003-2004]; **Royal Bank of Scotland Group**, Edinburgh, UK [2002]; **Halifax/Bank of Scotland**, Leeds, UK [2001]; **Banque Nationale de Belgique**, Brussels, Belgium [2001]; **Deutsche Bank Ltd.**, London, UK [2000-2001]; **Lloyds/TSB Bank Ltd.**, Southend-on-Sea & London, UK [2000]; **Bank One International/First USA Bank**, Cardiff, UK [1999]; **Générale de Banque**, Brussels, Belgium [1998-1999]; **Perot Systems Europe Ltd.**, Nottingham, UK [1997-1998]; **Chartered Trust Plc (Standard Chartered Bank)**, Cardiff, UK [1996-1997]; **Legal & General Assurance**, Kingswood, Surrey, UK [1996]; **Sun Life Assurance Company of Canada (UK) Ltd.**, Basingstoke, UK [1989-1993]; **Databank Systems Ltd.**, Wellington, NZ [1988-1989]

# Are Greenfield's Mythical?

Putting this in context…



# Are Greenfield's Mythical?

**New startups:**

None, zip, nadda…

**No security function or no security management function:**

1. Sun Life Assurance Company of Canada (UK) Limited [1989-1993]
2. Bank One International/First USA Bank [1999] *
3. Lloyds/TSB Bank Limited [2000]
4. Fonterra Co-operative Group Limited [2004-2005]
5. BT Syntegra Limited, London [2006]
6. Lateral Security (IT) Services Limited [2010-2012]
7. Health Benefits Limited [2013 on] *

* Up-and-running for less than 6 months at that time though...

# Are Greenfield's Mythical?

**Question:** *"So … is there any such thing as a greenfield security opportunity left in the wild?"*

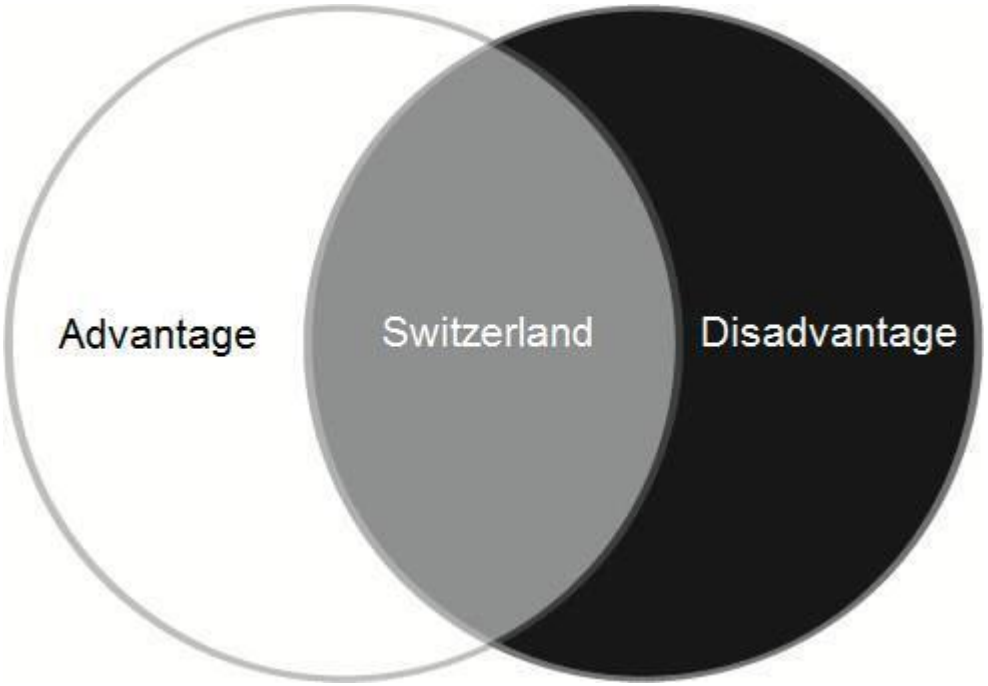

**Answer:** In my experience then? F'sure! But…

# Are Greenfield's Mythical?

**Question:** *"But ... if such mythical beasties do exist ... are they worth signing on for?"*


**Consultants' Answer:** *"Before answering that question … let's weigh up the pro's and con's…"*

# ADVANTAGES VS. DISADVANTAGES




**Note:** Much of what follows is applicable to anyone in IT. Whether developer, architect, security person … or CIO.

# Advantages vs. Disadvantages

**Greenfield advantages could include:**

- A new site with new technologies;
- Maximum flexibility in approach;
- Low maintenance due to not having to maintain existing or legacy systems;
- Having a hand in design and development around meeting current and future needs;
- An opportunity to build a company's image; and
- The ability to be more proactive in your approach.

# Advantages vs. Disadvantages

**Brownfield advantages could include:**

- Already-existing and mature environments;
- Infrastructure and support services already in place;
- Upgrade costs are cheaper than implementing new;
- The time frame for approvals is much shorter;
- Employees are already on-site, in-place, and settled into their positions; and
- More effective and efficient use of infrastructure.

# Advantages vs. Disadvantages

**Greenfield advantages could include:**

- A new site with new technologies;
- Maximum flexibility in approach;
- Low maintenance due to not having to maintain existing or legacy systems;
- Having a hand in design and development around meeting current and future needs;
- An opportunity to build a company's image; and
- The ability to be more proactive in your approach.

**Brownfield advantages could include:**

- Already-existing and mature environments;
- Infrastructure and support services already in place;
- Upgrade costs are cheaper than implementing new;
- The time frame for approvals is much shorter;
- Employees are already on-site, in-place, and settled into their positions; and
- More effective and efficient use of infrastructure.

# Advantages vs. Disadvantages

**Greenfield disadvantages could include:**

- Infrastructure and support services not in place yet;
- The time frame for approvals is much longer;
- Other areas of the business have a higher priority (especially financially);
- Cost-cutting due to new installations being more expensive;
- A lack of, and overstretched, employees; and
- High stress levels.

# Advantages vs. Disadvantages

**Brownfield disadvantages could include:**

- Environments only geared to meet current business requirements;
- Cost blow-outs due to size, complexity, and unforeseen circumstances;
- Infrastructure and systems already compromised;
- Legacy environments and systems;
- Implementation of new infrastructure and systems costly and time-consuming; and
- The silo mentality.

# Advantages vs. Disadvantages

**Greenfield disadvantages could include:**

- Infrastructure and support services not in place yet;
- The time frame for approvals is much longer;
- Other areas of the business have a higher priority (especially financially);
- Cost-cutting due to new installations being more expensive;
- A lack of, and overstretched, employees; and
- High stress levels.

**Brownfield disadvantages could include:**

- Environments only geared to meet current business requirements;
- Cost blow-outs due to size, complexity, and unforeseen circumstances;
- Infrastructure and systems already compromised;
- Legacy environments and systems;
- Implementation of new infrastructure and systems costly and time-consuming; and
- The silo mentality.

# Advantages vs. Disadvantages

There's an App for everything…

But now let's look at the reality…

# THE REALITY

# The Reality

**No security function or no security management function:**

1. Sun Life Assurance Company of Canada (UK) Limited [1989-1993]
2. Bank One International/First USA Bank [1999]
3. Lloyds/TSB Bank Limited [2000]
4. Fonterra Co-operative Group Limited [2004-2005]
5. BT Syntegra Limited, London [2006]
6. Lateral Security (IT) Services Limited [2010-2012]
7. Health Benefits Limited [2013 on]

# The Reality

1. **Sun Life Assurance Company of Canada (UK) Ltd. [1989-1993]**

*Position: (Permanent) Information Security Analyst*

- No prior security function (system programmers); and
- CA-ACF2 system in, but in logging mode only.

*Lessons: 'Lip-service' to security; incident; demotion followed*

From 'Greenfield advantages':

- *Low maintenance (due to a new installation);*
- *Having a hand in deployment (to meet current and future needs); and*
- *The ability to be proactive.*

From 'Greenfield disadvantages':

- *Other areas of the business having a higher priority.*

# The Reality

**2. Bank One International/First USA Bank [1999]**

*Position: (Contract) Data Security Analyst*

- No prior security function; and
- My first BS 7799 security policy.

*Lessons: No new security function appointed; bought by HBOS*

From 'Greenfield advantages':

- *A new site;*
- *Low maintenance (due to a new installation); and*
- *An opportunity to build the company's image.*

From 'Greenfield disadvantages':

- *A lack of, and overstretched, employees.*

# The Reality

**3. Lloyds/TSB Bank Ltd. [2000]**

*Position: (Contract) Security Consultant*

- No prior high-level security function; and
- Administration and excellent monitoring in place.

*Lessons: Bad audit; Group and the political situation*

From 'Greenfield advantages':

- *Having a hand in development (to meet current and future needs); and*
- *The ability to be proactive.*

From 'Greenfield disadvantages':

- *[None]*

# The Reality

**4. Fonterra Co-operative Group Ltd. [2004-2005]**

*Position: (Permanent) IS Security Manager*

- No prior high-level security function; and
- Security outsourced.

*Lessons: Contract analysis; 'empire-building'*

From 'Greenfield advantages':

- *Low maintenance (due to being outsourced);*
- *Having a hand in development (to meet current and future needs); and*
- *An opportunity to build the company's image.*

From 'Greenfield disadvantages':

- The time frame for approvals much longer; and
- Other areas of the business having a higher priority.

# The Reality

**5. BT Syntegra Ltd., London [2006]**

*Position: (Contract) Security Consultant*

- No prior high-level security function; and
- 'Decentralised' security model.

*Lessons: Similar to Telecom NZ; political situation; project failure*

From 'Greenfield advantages':

- Low maintenance (due to new-ish installations);
- Having a hand in development (to meet current and future needs); and
- An opportunity to build the company's image.

From 'Greenfield disadvantages':

- Infrastructure and support services not in place; and
- Cost-cutting due to new installations being expensive.

# The Reality

**6. Lateral Security (IT) Services Ltd. [2010-2012]**

*Position: (Contract) Senior Security Consultant*

- No prior high-level security function; and
- Business benefit.

*Lessons: Comply with everything (ISO/IEC, PCI DSS, NZISM, AGISM, ITIL, Cloud Alliance, etc.); learn to sell*

From 'Greenfield advantages':

- *Having a hand in development (to meet current and future needs);*
- *An opportunity to build the company's image; and*
- *The ability to be proactive.*

From 'Greenfield disadvantages':

- *A lack of, and overstretched, employees.*

# The Reality

**7. Health Benefits Limited [2013 on]**

*Position: (Contract) Security Lead*

And I won't be making any comments here … nope!

# The Reality

And … always … keeping in mind:


So … how does one cope with the reality then?

# COPING WITH THE REALITY


## The GCSB

**The only public service department that *now* really listens...**

# Coping With The Reality

Remember this?

*“Seeking an exciting new challenge? Want to be responsible for building and shaping an embryonic information security function? Then you so won't want to miss this golden opportunity!”*

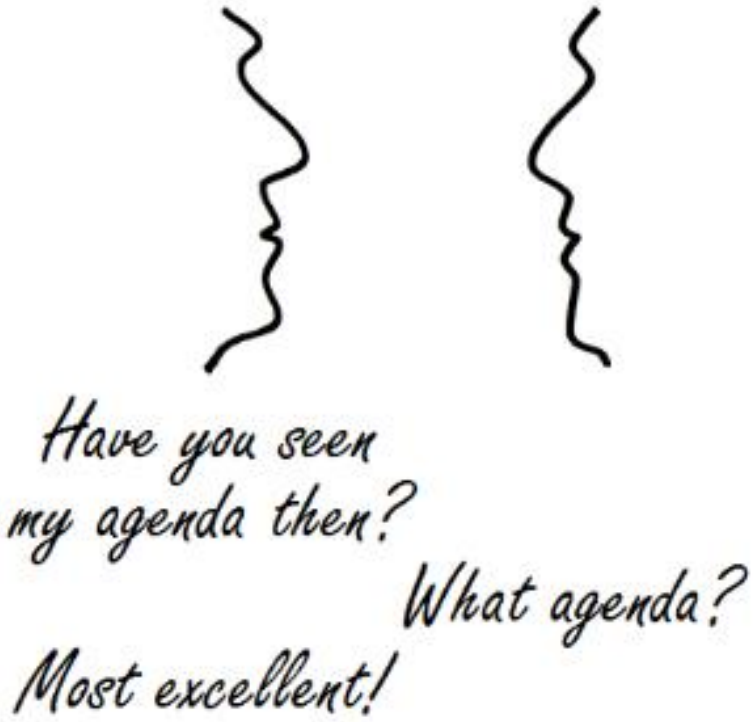
# Coping With The Reality

What C-level management say…


…and what they actually mean.

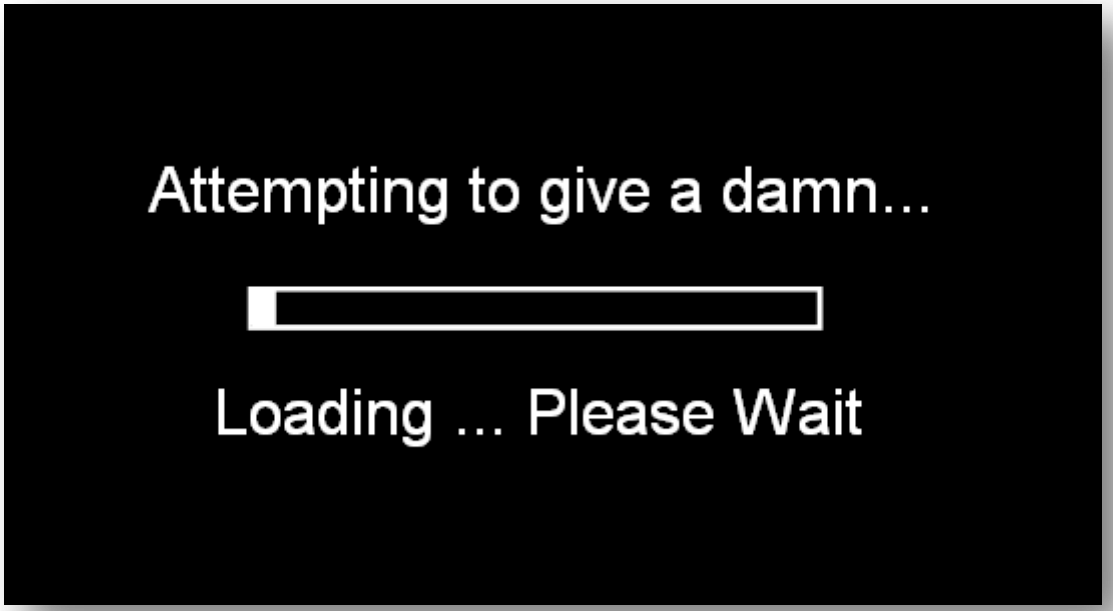
# Coping With The Reality

Be aware that management may have a hidden agenda…



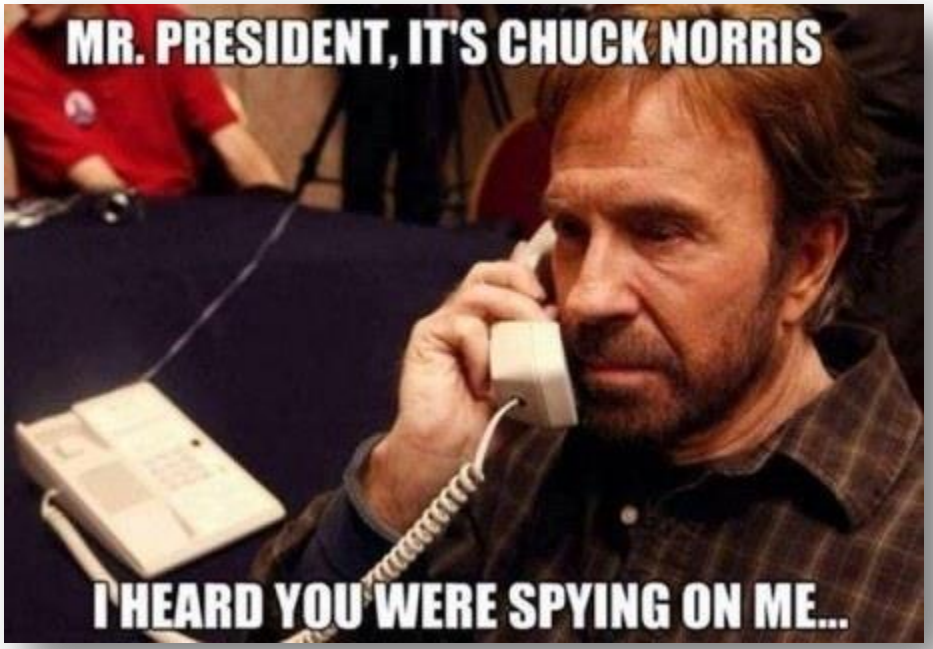
# Coping With The Reality

The tried-and-tested ‘insecurity through obscurity’ methodology…



# Coping With The Reality

Are you already too late?



# Coping With The Reality

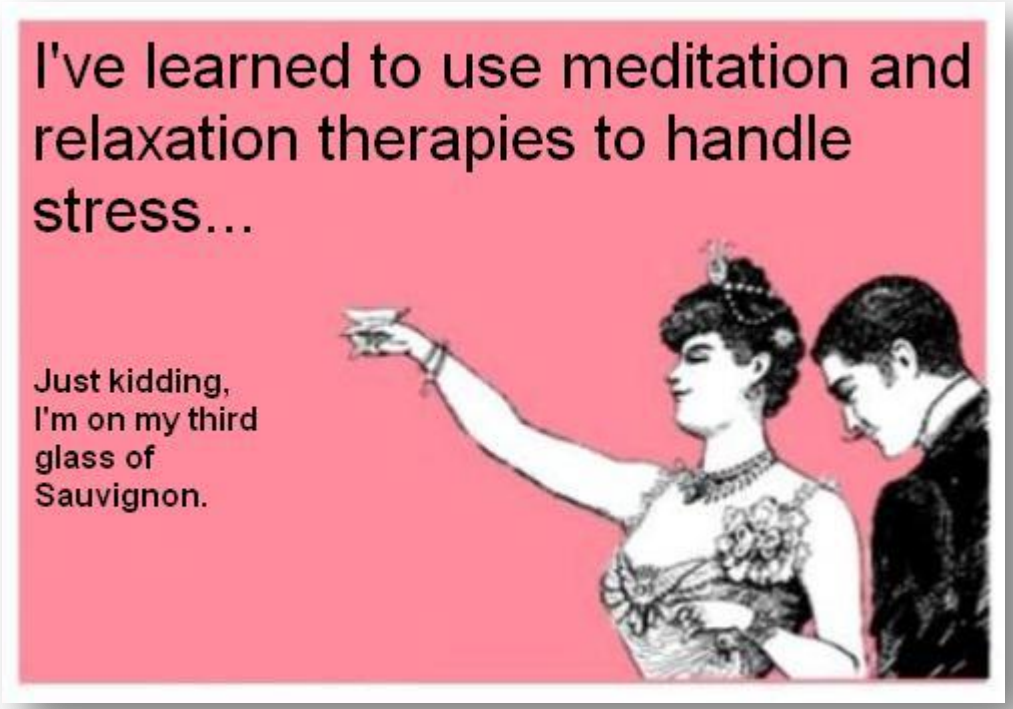
The extra complication of third party and/or out-sourced involvement…

# Coping With The Reality

Beware the ‘blanket statement’…

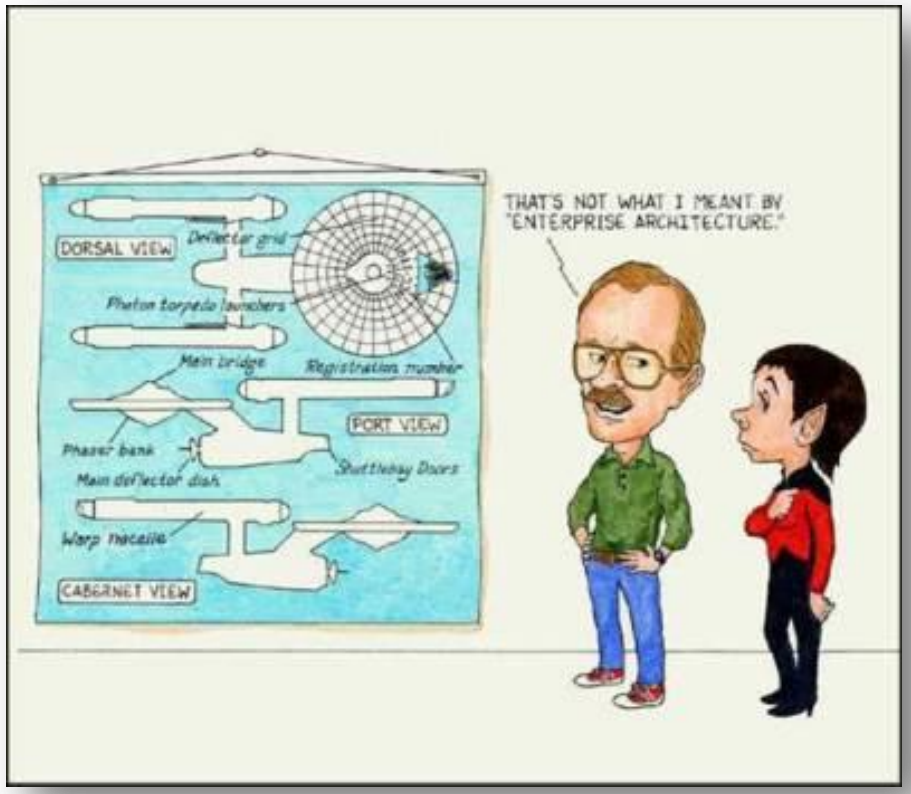
# Coping With The Reality

The stresses and pressures…



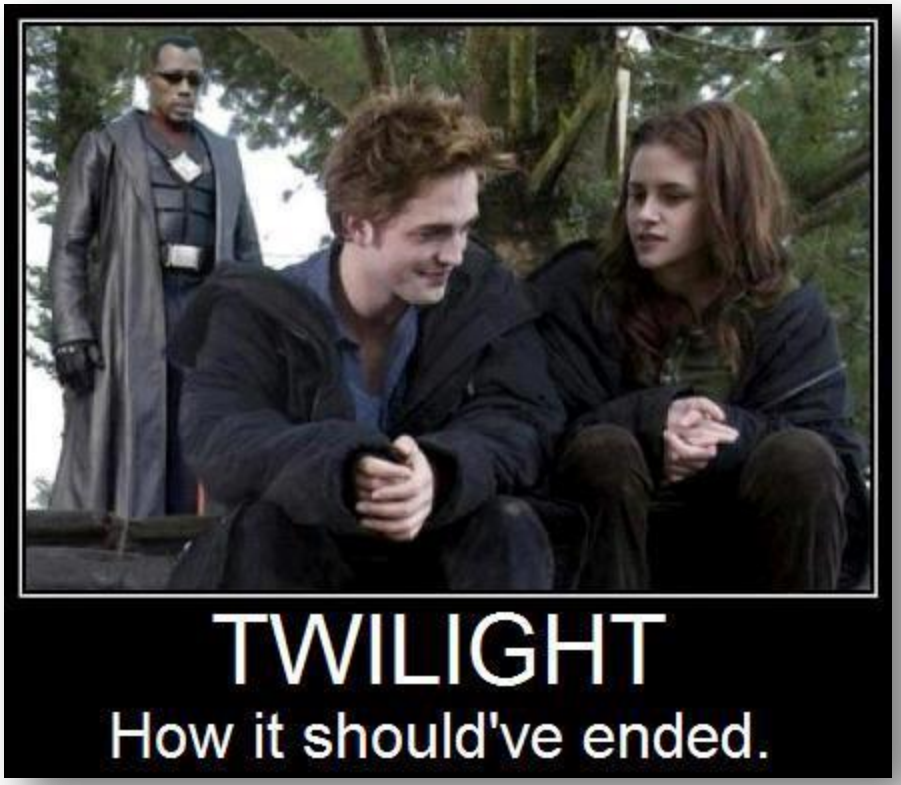
# Coping With The Reality

Architects, architects ... and more architects!



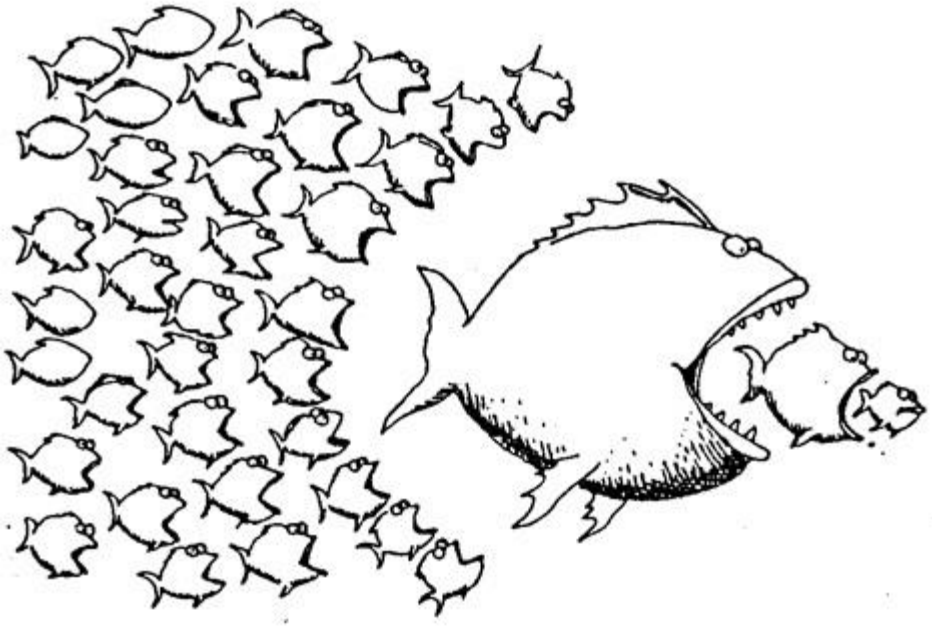
# Coping With The Reality

Handling the ‘precious’ people.’



# Coping With The Reality

The ‘top-down’ versus ‘bottom-up’ approach…



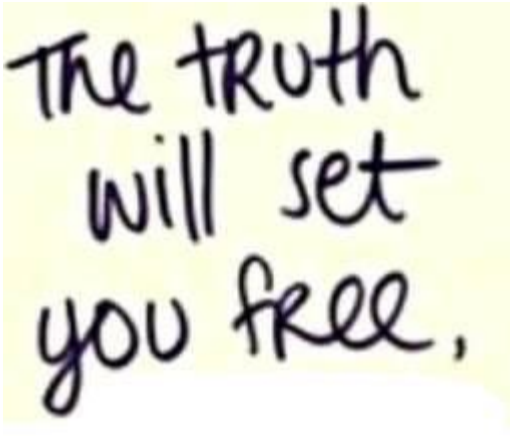
# Coping With The Reality

The ‘Keep It Simple, Stupid’ (KISS) principal…

# Coping With The Reality

Just some of the hurdles you need to overcome…

# SUMMING UP



# SUMMING UP

# Summing Up

This is how it all started: **"Seeking an exciting new challenge...?"**

- So is there any such thing as a greenfield security opportunity left in the wild? **Reckon**
- And ... if such mythical beasties do exist ... are they worth signing on for? **Reckon?**
- The pros and the cons of setting up of an information security function in an organisation from scratch ('Greenfield'); as opposed to trying to bed yourself down into an already-existing organisation ('Brownfield'). **Hopefully**

*So ... if you want to hear a guy speak who reckons he's forgotten more than he ever thought he knew? Then this is so the talk for you!* **Huh?**

# OWASP Bingo

- ✓ Grumpy Cat
- ✓ Graphs & Pie Charts
- ✓ Picard Facepalm
- ✓ Novopay
- ✓ The GCSB
- ✓ Bored Baby
- ✓ Chuck Norris
- ✓ Star Trek
- ✓ Twilight

*and*

# OWASP Bingo

- ✓ Grumpy Cat
- ✓ Graphs & Pie Charts
- ✓ Picard Facepalm
- ✓ Novopay
- ✓ The GCSB
- ✓ Bored Baby
- ✓ Chuck Norris
- ✓ Star Trek
- ✓ Twilight

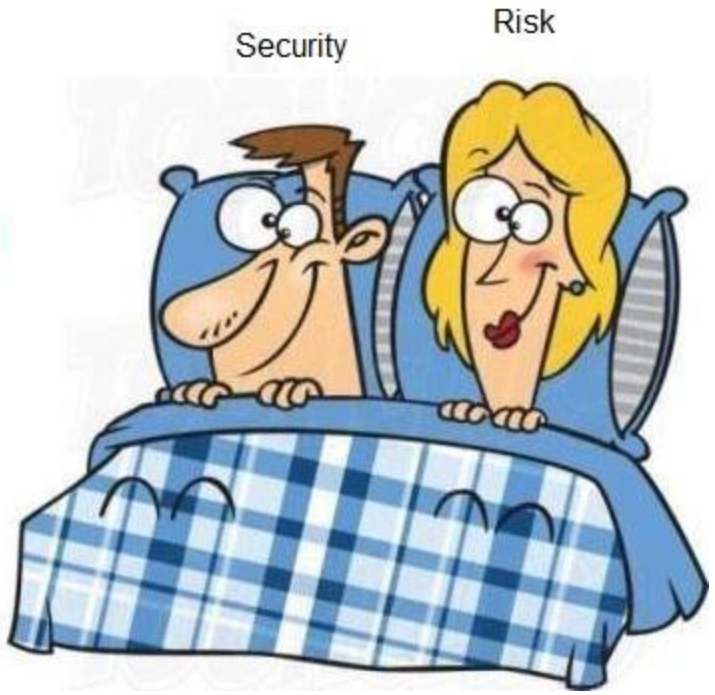
  *and*

- ✓ Wearing Pants…

# ‘Your Current Obsession…’

**“Anatomy Of Fraud: A Study Of Fraud In New Zealand”**

http://abkaye.blogspot.co.nz/

# Any Questions?