LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

Comply Or Die!

(Or 'Does Compliance Employ Techies Or Should Techies Employ Compliance?')

(How about 'How I Learned to Stop Worrying and Love Standards')

(Alternatively 'Gsus wtf aight? Tisl! Wtg4a\%/?')

Presenter: Andrew Kelly

Date: 30th June 2011

Place: ISIG, ~~Wellywood~~ Wellington

LATERAL | SECURITY

A PowerPoint Slide

LATERAL | SECURITY

An Oxymoron

This Slide Intentionally Left Blank

LATERAL | SECURITY

(IT Security) Places What I Have Worked

Lateral Security (IT) Services Ltd., Wellington, NZ [2010 on]; 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]

LATERAL | SECURITY

A Favourite Quote

'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.'

Bruce Schneier

LATERAL | SECURITY

Another Favourite Quote

'When you've got 'em by the balls, their hearts and minds will follow.'

Charles 'Chuck' Colson? Special Counsel for President Nixon. 1969-73

LATERAL | SECURITY

Think Outside The Square

On Monday 27th June 2011 the Hague-based International Criminal Court issued a warrant for the arrest of Colonel Gaddafi.

Accusing the Libyan leader of crimes against humanity.

LATERAL | SECURITY

Think Outside The Square

On Monday 27th June 2011 the Hague-based International Criminal Court issued a warrant for the arrest of Colonel Gaddafi.

Accusing the Libyan leader of crimes against humanity.

They've now limited Gaddafi's options:

1. He can't flee to Saudi Arabia (the traditional escape route for 'retiring' African and Middle East dictators);
2. He can't flee to most any other country; and
3. He now pretty much 'has to' fight to the bitter end?

That last option will almost certainly result in the deaths of more Libyan citizens (innocent or otherwise).

LATERAL | SECURITY

Think Outside The Square

'The Uninvited Guest: Chinese Sub Pops up in Middle of U.S. Navy Exercise, Leaving Military Chiefs Red-faced'

Daily Mail (UK), November 2007

When the U.S. Navy deploys a battle fleet on exercises, it takes the security of its aircraft carriers very seriously indeed.

At least a dozen warships provide a physical guard while the technical wizardry of the world's only military superpower offers an invisible shield to detect and deter any intruders.

That is the theory. Or, rather, was the theory…

LATERAL | SECURITY

Think Outside The Square

Uninvited guest: A Chinese Song Class submarine, like the one that surfaced by the USS Kitty Hawk

LATERAL | SECURITY

Wikipedia Definition

1. Compliance (mechanical science): the inverse of stiffness.
2. Compliance (medicine): a patient's (or doctor's) adherence to a recommended course of treatment.
3. Compliance (physiology): a measure of the tendency of a hollow organ to resist recoil toward its original dimensions upon removal of a distending or compressing force.
4. Compliance (psychology): the act of responding favourably to an explicit or implicit request offered by others.
5. Governance, Risk Management, and Compliance ('GRC'): an umbrella term covering an organisation's approach across these areas.
6. Regulatory Compliance: the act of adhering to, and demonstrating adherence to, a standard or regulation.

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

c. Raise this with the Board

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

c. Raise this with the Board

d. Put more defences in place to reduce the risk

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

c. Raise this with the Board

d. Put more defences in place to reduce the risk

e. All or any combination of the above

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

c. Raise this with the Board

d. Put more defences in place to reduce the risk

e. All or any combination of the above

Step 5: Your manager tells you your concern is being addressed

LATERAL | SECURITY

The Ideal

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide to:

a. Place this on the risk register as a high risk

b. Make funding available to address this risk

c. Raise this with the Board

d. Put more defences in place to reduce the risk

e. All or any combination of the above

Step 5: Your manager tells you your concern is being addressed

Step 6: You go to the pub...

LATERAL | SECURITY

The Ideal

And you feel good about yourself.

And that night you sleep the sleep of the goodly and righteous.

However...

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

c. This system is seen by the Board as 'business-critical' so...

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

c. This system is seen by the Board as 'business-critical' so...

d. Isn't this why we have defence-in-depth?

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

c. This system is seen by the Board as 'business-critical' so...

d. Isn't this why we have defence-in-depth?

e. All or any combination of the above

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

c. This system is seen by the Board as 'business-critical' so...

d. Isn't this why we have defence-in-depth?

e. All or any combination of the above

Step 5: Your manager tells you your concern is being ignored

LATERAL | SECURITY

The Reality

Step 1: You uncover a major security flaw in one of your company's information processing facilities

Step 2: You immediately bring this to your manager's notice - who agrees this is indeed a cause for concern

Step 3: Your manager decides to raise this risk with even more senior management - so approach *their* manager

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. This risk is acceptable as your company has a high risk tolerance

b. No funding is available at this time to address this risk

c. This system is seen by the Board as 'business-critical' so...

d. Isn't this why we have defence-in-depth?

e. All or any combination of the above

Step 5: Your manager tells you your concern is being ignored

Step 6: You go to the pub...

LATERAL | SECURITY

The Reality

And you feel unhappy with the world.

And that night you sleep the sleep of the inebriated and restless.

However...

LATERAL | SECURITY

The ‘Real’ Reality

...

Step 4: Their manager agrees this is indeed a cause for concern - and they decide:

a. To place this on the risk register as a high risk ... knowing this risk will be seen as acceptable as your company has a high risk tolerance

b. Make funding available to address this risk ... in the next financial year

c. Raise this with the Board ... knowing this system is seen by the Board as ‘business-critical’ so...

d. Put more defences in place to reduce the risk ... by signing-off on that long-delayed upgrade to the firewall

e. All or any combination of the above

Step 5: Your manager tells you your concern is being addressed

Step 6: You go to the pub...

LATERAL | SECURITY

The ‘Real’ Reality

And you feel content with the world.

Kind of.

And that night you sleep the sleep of the almost-goodly and semi-righteous.

Which is somehow worse than feeling unhappy with the world...

LATERAL | SECURITY

Can Compliance Make You Safe?

LATERAL | SECURITY

An Example

SAN's September 2009 **'The Top Cyber Security Risks'** article:

Two Risks Dwarf All Others, But Organizations Fail To Mitigate Them

Featuring attack data from TippingPoint intrusion prevention systems protecting 6,000 organizations, vulnerability data from 9,000,000 systems compiled by Qualys, and additional analysis and tutorial by the Internet Storm Center and key SANS faculty members.

Priority One: Client-side Software That Remains Unpatched

Waves of targeted email attacks ... are exploiting client-side vulnerabilities in commonly used programs ... On average, major organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities.

Priority Two: Internet-facing Web Sites That Are Vulnerable

Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet ... Most web site owners fail to scan effectively for the common flaws...

LATERAL | SECURITY

Priority 1: Client-side Software

What do we have to - or can we - comply with here?

AS/NZS ISO/IEC 27002 [ISO 27002]:

- 6.1.7 Contact with special interest groups
- 12.4.1 Control of operational software
- 12.5.2 Technical review of applications after operating system changes
- 12.5.3 Restrictions on changes to software packages
- 12.6.1 Control of technical vulnerabilities

PCI Data Security Standard (v2.0) [PCI DSS]:

Requirement 6: Develop and maintain secure systems and applications [specifically subsections 6.1 and 6.3.1]

NZ Information Security Manual (v1.0) [NZISM]:

- 4.5. Standard Operating Procedures
- 12.1. Product

LATERAL | SECURITY

Priority 1: Client-side Software

NZISM (continued):

- 12.2. Product Installation and Configuration
- 12.4. Product Patching and Updating
- 14.1. Standard Operating Environments
- 17.6. Intrusion Detection and Prevention

Security in the Government Sector (2002) [SIGS]:

- Configuration Management
- Annex A - Minimum Standards for Internet Security in the New Zealand Government

Control Objectives for Information and Related Technology (v4.1) [COBIT]:

- AI3.3 Infrastructure Maintenance
- AI6 Manage Changes
- AI6.1 Change Standards and Procedures

LATERAL | SECURITY

Priority 1: Client-side Software

COBIT (continued):

- DS5.9 Malicious Software Prevention, Detection and Correction
- DS8 Manage Service Desk and Incidents

Information Technology Infrastructure Library (v3.0) [ITIL]:

- SO 5.4 Server Management and Support
- SO 5.5 Network Management
- SO 5.9 Desktop Support
- SO 6.5.5 Application Management generic activities
- SO 7.1.4 Discovery/Deployment /Licensing technology
- SO 8.1.1 Change triggers
- CSI 7.1.2 Systems and network management

LATERAL | SECURITY

Priority 1: Client-side Software

IT Control Objectives for Sarbanes-Oxley (the IT Governance Institute) [SOX]:

Manage Changes (AI6, AI7)

LATERAL | SECURITY

Priority 2: Internet-facing Web Sites

What do we have to - or can we - comply with here?

AS/NZS ISO/IEC 27002 [ISO 27002]:

- 6.1.6 Contact with authorities
- 10.4.1 Controls against malicious code
- 10.9.1 Electronic commerce
- 12.2.1 Input data validation
- 12.5.4 Information leakage
- 12.6.1 Control of technical vulnerabilities
- 13.1.1 Reporting information security events
- 15.2.2 Technical compliance checking

PCI Data Security Standard (v2.0) [PCI DSS]:

- Requirement 11: Regularly test security systems and processes [all five subsections]

LATERAL | SECURITY

Priority 2: Internet-facing Web Sites

NZ Information Security Manual (v1.0) [NZISM]:

- 7.3. Managing Cyber Security Incidents
- 9.4. Using the Internet
- 14.1. Standard Operating Environments
- 14.3. Web Applications
- 14.6. Web Application Development
- 18.4. Firewalls

Security in the Government Sector (2002) [SIGS]:

- Malware Protection Standards
- Configuration Management
- Internet Security
- Internet Server Configuration Standards

LATERAL | SECURITY

Priority 2: Internet-facing Web Sites

Control Objectives for Information and Related Technology (v4.1) [COBIT]:

- PO6 Communicate Management Aims and Direction
- AI7 Install and Accredit Solutions and Changes
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS13 Manage Operations

Information Technology Infrastructure Library (v3.0) [ITIL]:

- SD 4.6 Information security management
- SD 9 Challenges, Critical Success Factors and risks
- ST 9 Challenges, Critical Success Factors and risks
- SO 3.2.4 Reactive versus proactive
- SO 4.1.4 Policies/principles/basic concepts

LATERAL | SECURITY

Priority 2: Internet-facing Web Sites

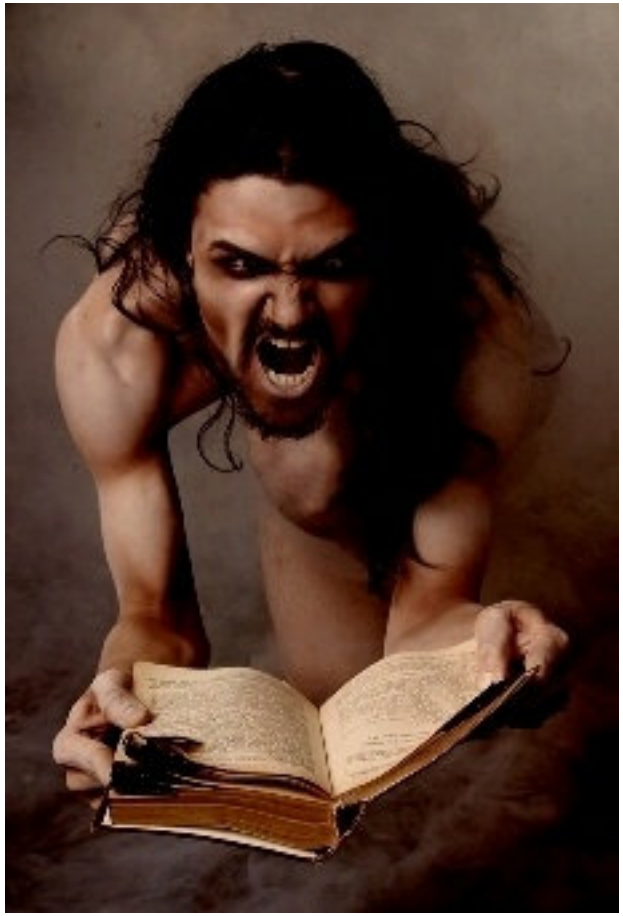
ITIL (continued):

- SO 5.11 Internet/Web Management
- SO 6.3.4 Technical Management organization
- SO 7.2 Event Management

LATERAL | SECURITY

How To Use This

So, how to scare *your* manager with … compliance



LATERAL | SECURITY

Make it Personal

Question: ‘So why don’t senior and/or ‘C-level’ management appear to take any notice of gaping holes in their security infrastructure?’

LATERAL | SECURITY

Make it Personal

Question: ‘So why don’t senior and/or ‘C-level’ management appear to take any notice of gaping holes in their security infrastructure?’

One Answer: ‘Because ... it ain’t personal!’

LATERAL | SECURITY

Make it Personal

The object here is to shrink these…

LATERAL | SECURITY

Make it Personal

To the size of these…

LATERAL | SECURITY

How?

You're working for an outsource or vendor company:

Check if your company must comply with your client's IS Policy (or similar), any other standards (i.e.: PCI DSS, NZISM, ITIL), and/or a Contract

You have outsourcers and/or vendors:

Check if they must comply with your company's IS Policy, any other standards, and/or a Contract

You are bidding/will bid for a contract:

Check if your company will have to comply with their company's IS Policy, any other standards, and/or a Contract

You're working for a financial services company:

You just gotta comply with something, learn to live with it

You're working for a government department/SOE:

You just gotta comply with NZISM and ... lucky you

LATERAL | SECURITY

Example 1: Outsourcer

Schedule 2: IT Processes Statement of Work

4. INCIDENT MANAGEMENT

4.2(e) - X must implement an Incident Management process that assigns end-to-end responsibility and ownership of each incident to a single member of their support personnel;

4.3(b)(ii) - X must ensure the 'Incident Management System' provides a 'Unified Knowledge Database' that captures, stores, indexes, is searchable and retrieves information and solutions for reuse by X and Y in relation to incidents;

4.3(d) - X must provide Y users with access to the 'Incident Management System' and the 'Unified Knowledge Database';

4.3(e) - X must provide Y users with appropriate training in the proper use of the 'Incident Management System'; and

4.7(a) - X must develop and periodically update escalation procedures and (subject to Y's review and approval) distribute the procedures to Y users.

LATERAL | SECURITY

Example 2: Outsourcer

Regarding Incident Management, X must:

- Use system tools to automate alert management to reduce cost and free up valuable resources for Incident identification and Resolution;
- Detect and fix incidents before they turn into unplanned downtime;
- Implement a knowledge database;
- Identify and document, for distribution to Y stakeholders, the escalation triggers (e.g.: 15 minutes after a Severity Level 1 Problem is reported) that govern the tasks to be executed to meet SLAs;
- Assign severities in accordance with any guidelines issued by Y;
- Share Incident descriptions with Y to demonstrate the possible symptoms of an Incident and its impact on business;
- Provide the Services in accordance with any escalation triggers adopted by Y, as part of the governance processes;
- Develop escalation procedures for Severity Level 1 and 2 Incidents;
- Prepare a list of Y stakeholders to enable relevant parties to be kept informed in a timely manner; and
- Provide adequate information to other service providers, Y business units and End Users in the progress of their Resolution activities.

In Conclusion

- Be creative! Think outside of the box/square/whatever

LATERAL | SECURITY

In Conclusion

- Be creative! Think outside of the box/square/whatever
- Make - keep - it personal

LATERAL | SECURITY

In Conclusion

- Be creative! Think outside of the box/square/whatever
- Make - keep - it personal
- ‘The sky is falling on our heads here’

LATERAL | SECURITY

In Conclusion

- Be creative! Think outside of the box/square/whatever
- Make - keep - it personal
- ‘The sky is falling on our heads here’
- Audit ... is your BFF

LATERAL | SECURITY

In Conclusion

- Be creative! Think outside of the box/square/whatever
- Make - keep - it personal
- ‘The sky is falling on our heads here’
- Audit ... is your BFF
- Risk ... is BFF TBA?

LATERAL | SECURITY

In Conclusion

- Be creative! Think outside of the box/square/whatever
- Make - keep - it personal
- ‘The sky is falling on our heads here’
- Audit ... is your BFF
- Risk ... is BFF TBA?
- Learn ‘Office Politics 101’

LATERAL | SECURITY

Contact Details

Wellington 38-42 Waring Taylor Street
Petherick Tower, level 7
PO Box 8093
The Terrace, Wellington 6143
Phone: +64 4 4999 756

Auckland 187 Queen Street
Landmark House, level 8
PO Box 7706
Wellesley Street, Auckland
Phone: +64 9 377 0700

Presenter andrew.kelly@lateralsecurity.com
Web www.lateralsecurity.com

LATERAL | SECURITY