


IT 360 Canada



Unstructured Data Are You Paranoid Enough Yet?

Anton J Aylward
CISSP, CISA



System Integrity



Security... In the era of...

- The Perimeterless Organisation
- Mobile Computing
- 'The Cloud'
- Personal Devices



**Data is the
Lifeblood of
Business**

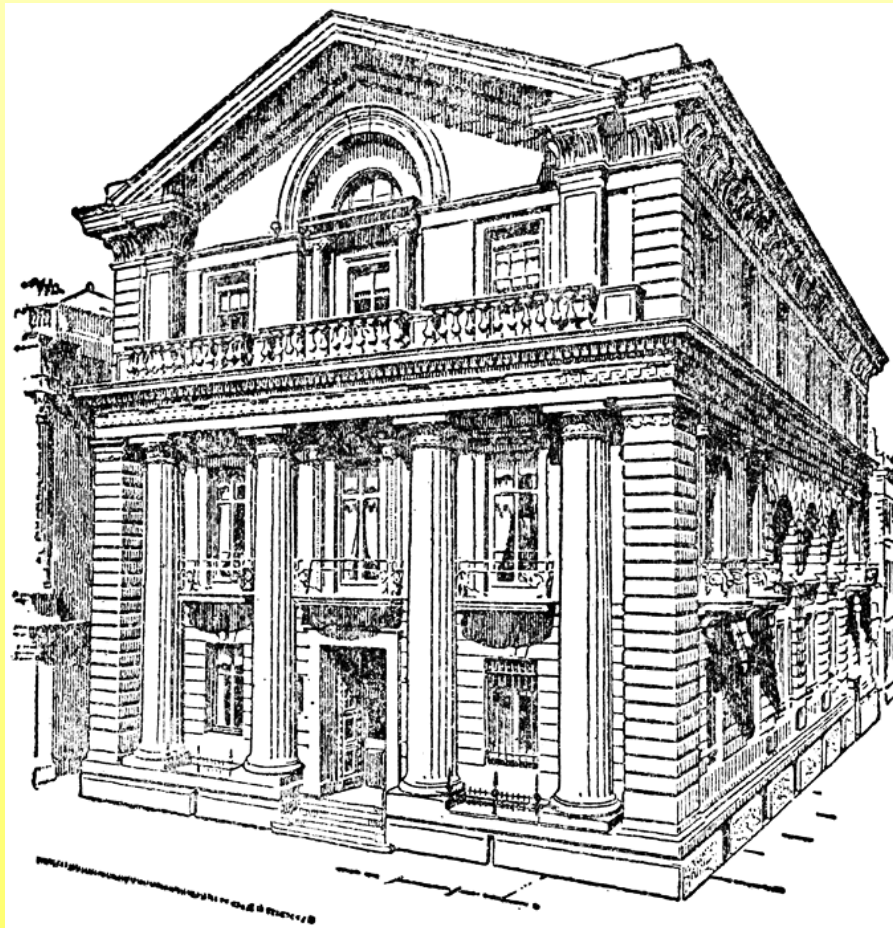


Data is the Lifeblood of Business

So where is this
data?



Consider a Bank





What is in its vaults?



Cash or Data?





Consider a Bank

- It has only ONE authoritative copy of your account information

*No matter how many printout,
remote access, branch copies*

- It has only ONE authoritative copy of your account information

Where is the Data for **YOUR** Business?



- On Personal Devices
 - “In the Cloud”
 - Outsourced
 - Data Vault
 - Backup
 - Hard Copy
- ❑ *If you don't now where your data is you don't have control over it*
 - ❑ *If there's more than one copy how do you know which is the right one?*
 - ❑ *How do you deal with Changes?*
 - ❑ *Who is authorized?*



What's on Your “Personal” Device?

- Your Identity
 - Name Address Phone
 - SIN#
 - Bank Information
 - Passwords
- Corporate Info
 - Passwords
 - People
 - Lots of data! !

Suppose you lost that



Is your 'Personal' Device Yours or the Company's?



What would it take to replace it?

- Is this your own or a corporate device?
- Is there a 'remote erase' mechanism?
- Did you make a backup?
- Do you need to cancel CC information?
- Do you need to change passwords?

Is your 'Personal' Device Yours or the Company's?



What would it take to replace it?

**Who is responsible if you
don't have a centralized
and managed IT
Department?**



Insider Threats

- Portable Devices
 - Smart phones
 - Laptops/Netbooks
 - USB devices
- Personal Devices
- Unauthorized Access
- Poor Awareness
- Malice
- File Sharing
- Rogue Wi-Fi/Modem
- Downloading
 - Malware
 - Unlicensed Media
- Data leaks
 - Blogging
 - E-Mail
 - IM/SMS

Do You ...

Have You ... Are You



- ✓ A laptop
 - ✓ A smartphone
 - ✓ A netbook

 - ✓ Use Windows®
 - ✓ Use MAC OSX
 - ✓ Use Linux/BSD
- ✓ Work from home
 - ✓ Work away from the office
 - ✓ Use E-Mail
 - ✓ Use a 'Portal'
 - ✓ Do Internet banking
 - ✓ Buy via the 'Net'
 - Amazon, EBay

Do You ...



Have You ... Are You

- ✓ Use
 - ✓ Internet Explorer or Firefox
- ✓ Use
 - ✓ SpamAssassin
 - ✓ Anti-Virus
- ✓ Block web adverts
- ✓ Purge your cache
- ✓ Drive a Toyota or Audi
- ✓ Use Internet Banking
- ✓ Download 'Media'
- ✓ Use Facebook
- ✗ Been Hacked
- ✗ Had your ID stolen



What's The Problem?

- Technology is **NOT** the problem
- People are the problem
- Technology is **NOT** the solution
- Changing behaviour is the solution



Pause

Mid Session Wave

STRETCH



Part Two

What to do About it

- Stop Leakage
- Protect yourself
- Protect the Company



① Policy

- People need to know what's expected of them
- Basis for Decisions, Budget, Planning
- Basis for Training, Discipline
- Basis for Products, Quality

① Policy



Writing Policy is Easy

Writing Good Policy is
hard



① Policy

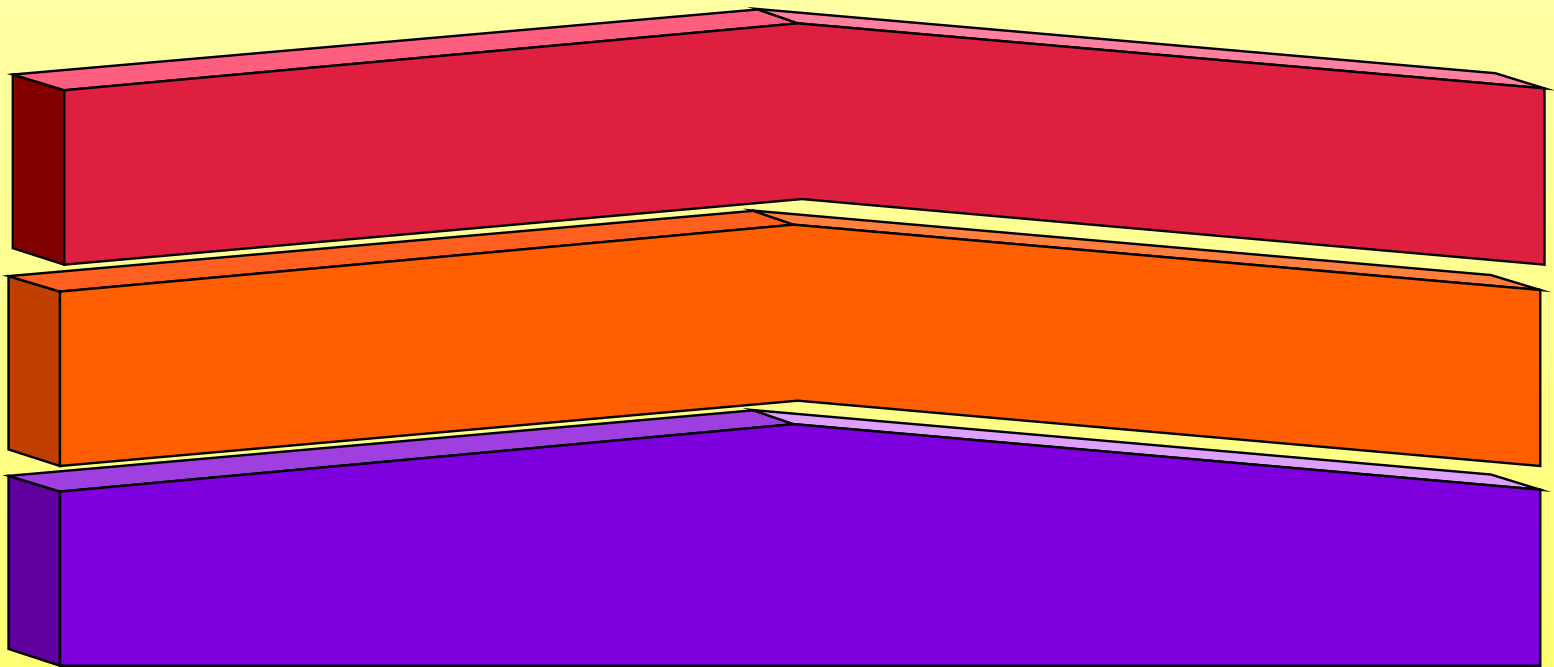
- Easy to understand
 - Unambiguous
 - General
 - Justifiable
 - Implementable
 - Enforceable
- *“Does it Apply to me?”*
 - *What am I Supposed to Do?*





① Policy

Policy Starts from the Top





② **Awareness**

- Purpose: Change Behaviour
- Part of a coherent plan
- Broaden perspective
- Be practical - Apply theory
- Measure and Improve



③ Good Practice

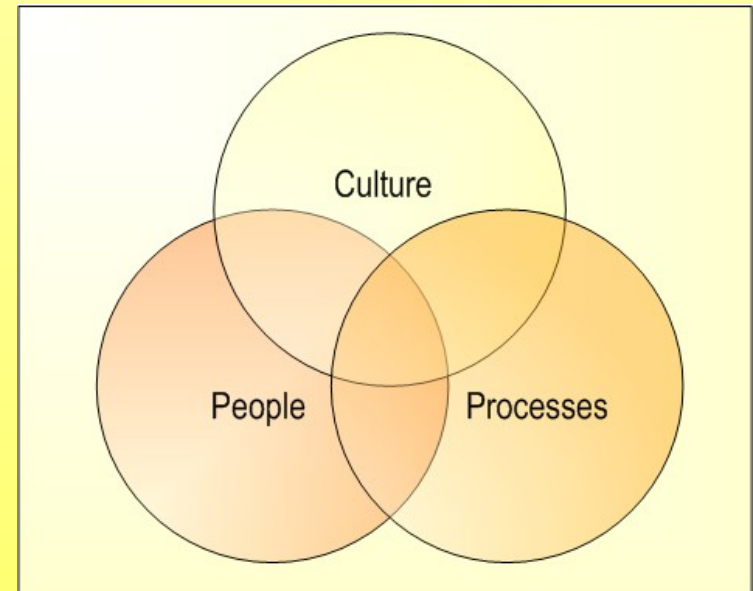
- The #1 Security Practice for Avoidable Incidents:

Change Management

- *The company changes ...*

Next most effective:

- ✓ Logging
- ✓ Data Classification
- ✓ Incident Response ...



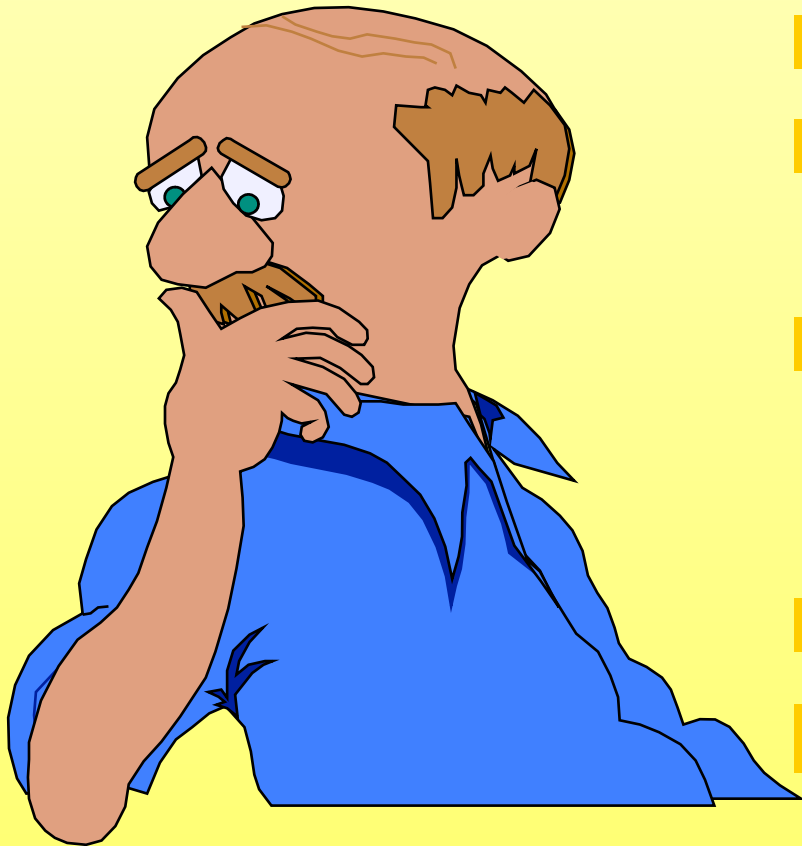


④ Logging

- Log Everything
- Establish patterns of normal use
 - Look for exceptions
- Develop Incident Response
- This is more "*Awareness*"



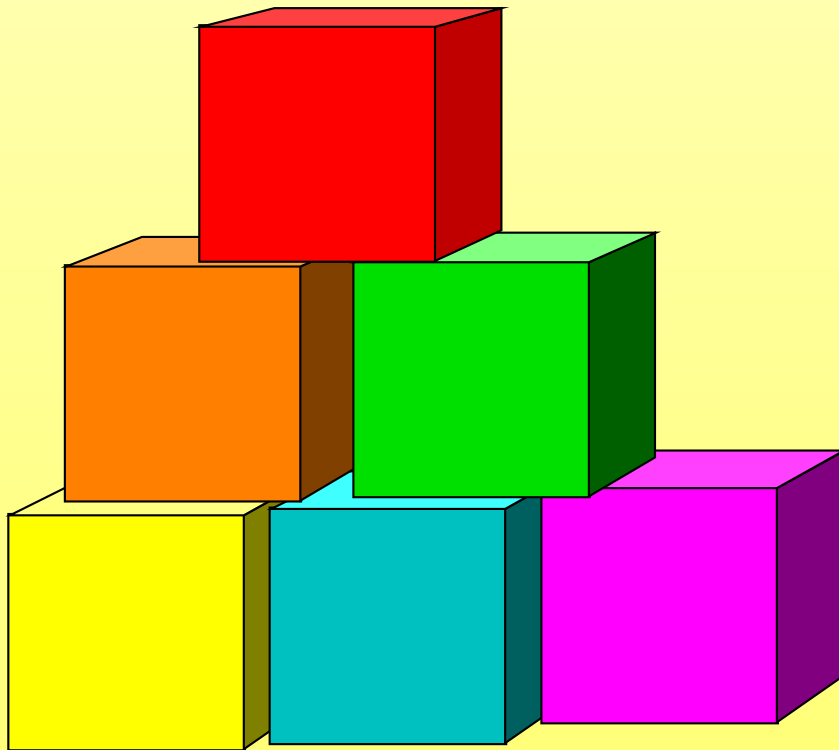
⑤ Be Paranoid



- Assume there is a flaw
- Don't accept vendor reassurances
- Track risk sites
 - SANS@RISK
 - Secunia
 - Blogs
- Network
- Be "Aware"



Five Points to Take Away



Be Aware
Be Proactive
Establish a Baseline
Log and Monitor
Don't rely on
Technology



Remember this ...

- ① Be Aware - Be Paranoid
 - ❑ Be proactive about learning Security
 - ❑ Don't trust vendor assurances
 - ❑ Spread Awareness



Remember this ...

- ② Be Proactive not Reactive
 - ❑ Plan for things to go wrong
 - ❑ Address Incidents not Disasters
 - ❑ Have Multiple Contingencies
 - ❑ Exercise & Practice



Remember this ...

③ Establish a Baseline

- Use Proven “Good Practices”

 - There is no Best Practice

Context Is Everything

- Continuous Improvement



Remember this ...

- ④ LOG. Monitor the Logs
 - ❑ Establish 'Normal' Conditions
 - ❑ Identify and react to anomalies

Context Is Everything



Remember this ...

- ⑤ You Can't Address Security With Just Technology
 - ❑ You need to change your people
 - ➔ Awareness
 - ❑ You need to change your business
 - ➔ Processes
 - ➔ Practices

Summary



Data - Corporate and Personal - doesn't exist just in databases under the supervision of IT staff, behind firewalls.

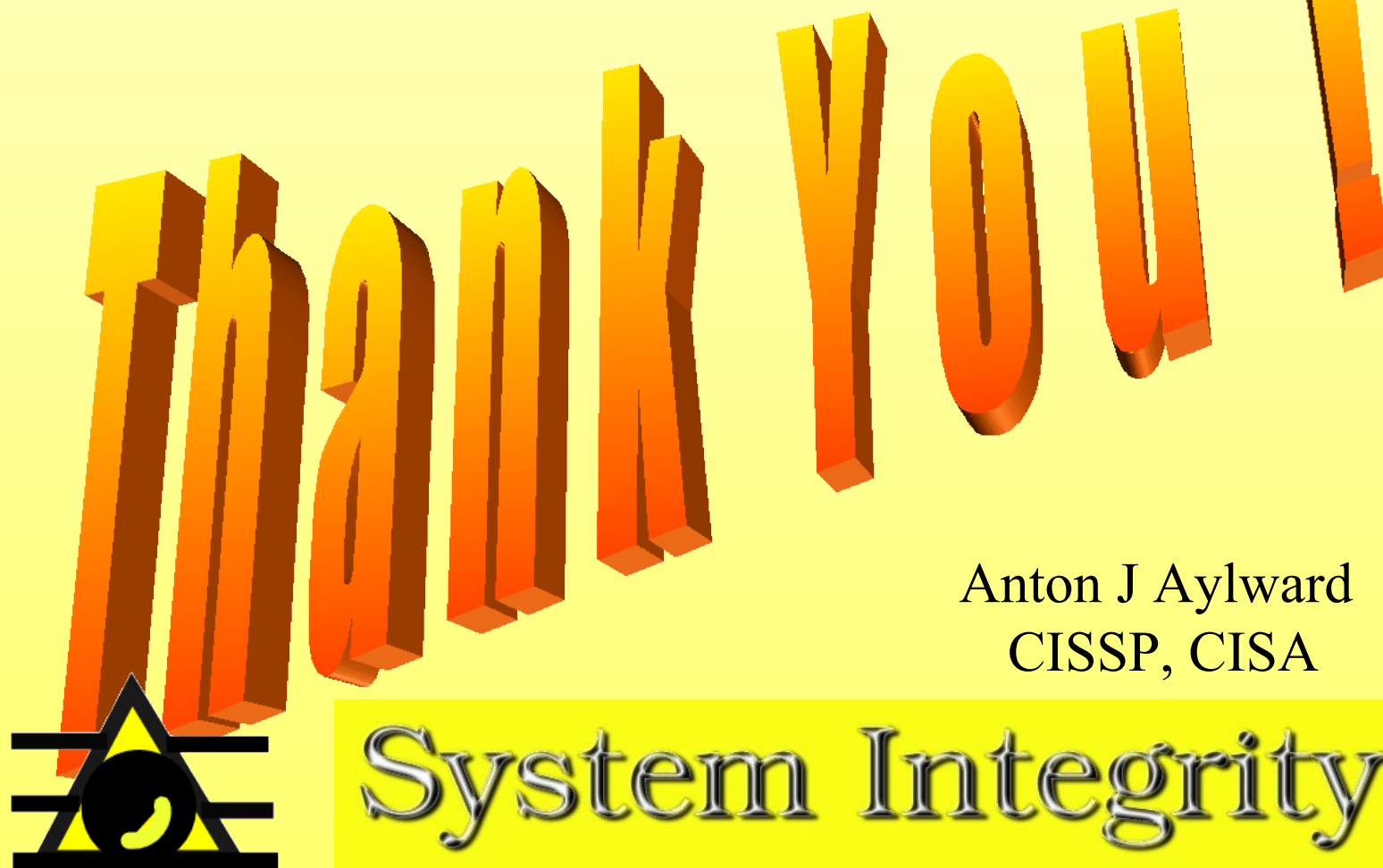
Its everywhere. Your laptop, smartphone, CDs, USB.
Its everywhere. The Cloud, the 'Net

Unstructured.
Ungoverned.

At Risk



IT 360 Canada



Anton J Aylward
CISSP, CISA



Download this presentation

www.infosecblog.antonaylward.com/presentations



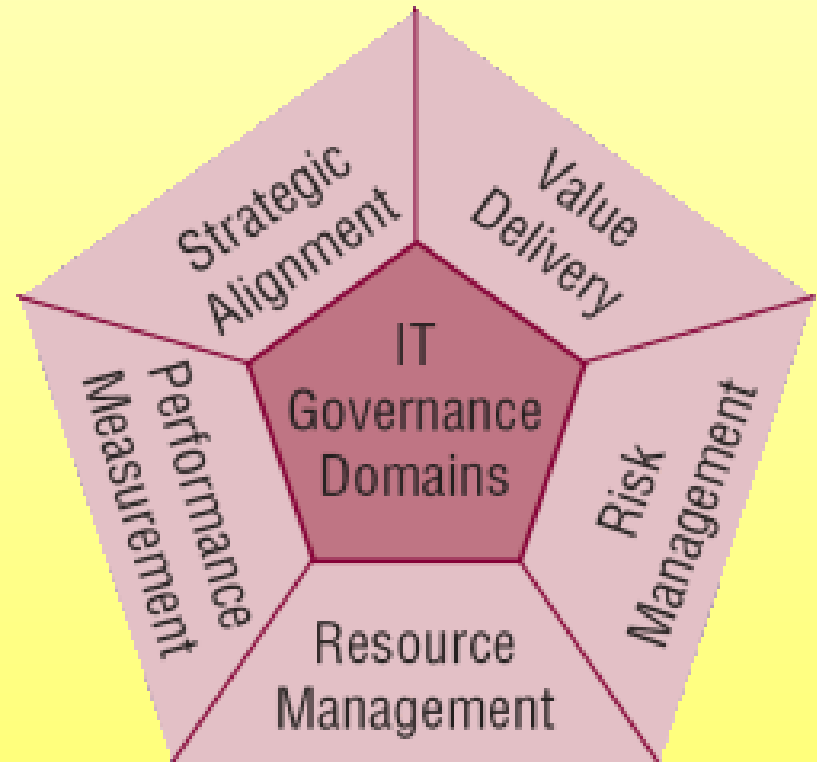


Who is this guy?

CISSP #4350 June 1997

CISA #113160 June 2002

- ▶ Governance, Policy & Risk Management
- ▶ Operations and Audit
- ▶ CobIT ValIT RiskIT
- ▶ ISO-27001 Policy & ISMS
- ▣ Founded Ontario's First ISP
- ▣ Board of Toronto Chapter of ISSA





Contact Information



System Integrity

“Security is not something that comes in a self-contained box. It requires a conscientious and continuous commitment that permeates every aspect of your enterprise and strategies. It is about understanding risks and managing them”

Anton J Aylward, CISSP CISA

aja@System1.ca

P: (416) 497-0201

C: (416) 509 9649

[http:// InfoSecBlog.AntonAylward.com](http://InfoSecBlog.AntonAylward.com)