evolve north

Data Security's best kept secret….

Mobile and Remote Working

"The Information Governance Challenge"

Mark Dennis – Evolve North

St James Park

25th October 2012

Delivered by evolve north

Evolve North

- IT Security and Information Governance Consultancy
  - 50/50 split between IT Security and Governance
  - Based in the North of England
  - UK wide client base - Public and Private sector
  - Solutions include Encryption, Remote Access, Identity Management, Strong Authentication, Web and Email, MDM, Firewall, UTM etc.
  - Information Governance consultancy around Data Protection Act, NHS Toolkit, Co Co, ISO27001, ISMS, PCI DSS, BYOD, Business Continuity etc.
  - Current projects…….

Delivered by evolve north

Clients

- Public and Private sector
  - Northern Strategic Health Authority, Durham PCT, Malmaison, Hotel Du Vin, NSS Scotland, City Hospitals Sunderland, Northumbria NHS Healthcare Foundation Trust, Barnardoes, Sintons, Rotherham PCT, NYPCT, Hadaways, County Durham and Darlington Foundation Trust, NHS Direct, Hull University, Askham Bryan College, Darlington Building Society, BSI, Calderdale NHS Trust, TSG, Phoenix, SBL, Bury College, States of Guernsey, Futures Housing, Chep, Islington Borough Council, Avarto, Sefton Borough Council, North Riding Council, 1st for Scotland, Queen Ethelburgs College, Wycombe Abbey, Southern Strategic Health Authority, North Lincs NHS Trust, Trustmarque, Middlesbrough PCT, Northumbria Mental Health Trust, Northumbria Police, Darlington and Stockton Borough Council, Switch IT, South of Tyne PCT, Avon and Wiltshire PCT……

Delivered by evolve north

Agenda

- The current compliance environment
- Working practices and changing attitudes
- New Governance
- Risk Assessment and Education
- BYOD (bring your own device)
- The Six Steps
- Last thoughts

Delivered by evolve north

- **The current compliance environment**
  - ICO – The Information Commissioner's view
    - Areas of Focus
      - NHS
      - Local Gov.
      - Criminal and Justice
      - Mobile and Remote Working
    - Areas of Concern
      - Control of Data
      - Data Leakage
      - Data Migration
    - Implications
      - Fines – lots of fines

Its getting tougher and the challenges are getting bigger

Delivered by evolve north

- **Working practices and changing attitudes**
  - We live in a 24 x7 connected world – its getting faster (4G)
    - Home Working
      - Becoming very common
      - More and more businesses moving in this direction
      - The home presents many new governance challenges
    - Mobile Working
      - We all do it to some degree
      - Often in public – Costa, Trains, Planes etc.
      - BYOD – new challenges
    - Generation X and Generation Y
      - We have very different views on personal data
      - Protected by the size of the flock….
      - Generation Y are now becoming Senior Management
      - We have to give them some slack

Delivered by evolve north

- **New Governance**
  - Bit like New Labour (reaching out to more people?)
    - Scope
      - Previously “in the building” now out in the wild
      - Involves IG, IT, HR, Legal and Senior Management
      - Legal contracts may be required rather than “policy”
      - PIA – Privacy Impact Assessment's
    - Cooperation
      - Its not IG or IT’s problem, responsibility etc.
      - It is a whole business responsibility
      - Risks must be identified and accepted by all involved
    - We can not be the “naysayers”
      - The world is changing
      - Peoples expectations are changing
      - Business is changing

    Its not easy…….

Delivered by evolve north

- **Risk assessment and education**
  - Risk assessment
    - Why?
      - It removes –
        - Opinion
        - Urban myths
        - Half truths
        - Rubbish written in BLOGs
        - Subject experts (we all have them)
        - I could go on all day
      - It introduces
        - Consistency
        - Objectivity
        - It puts it into “plain English”
        - Its not perfect – but it’s a lot better than anything else
      - If you use it religiously – it <u>will</u> save you at some point

      If you need some basic guidance just email me

Delivered by evolve north

- **Risk assessment and education (Continued)**
  - Education
    - Why?
      - Don’t assume –
        - People understand (at all levels)
        - People care
        - They believe you!
        - IT, IG, HR, Legal, Senior management are on the same page
        - Senior management actually know what's going on
        - The IT Department don't forward corporate email to Gmail/Hot Mail? or do anything else stupid!
        - Anything
      - Take every opportunity to educate – but don’t preach

      But if you want to be popular don’t work in IG or IT Security

Delivered by evolve north

- **BYOD**
  - Bring Your Own Device
    - Technically
      - Can be done –
        - MDM, NAC, Wi-Fi can now cope but only just
        - You will probably have to “touch” personal devices
        - Not all devices can be accepted
        - Not all will be able to use their mobile devices
    - Governance
      - Can be done – (but not easy)
        - Requires a complete re evaluation of current Governance approaches
        - Will need significant input from HR
        - Will require legal advice
        - PIA will need to be executed
        - Not all staff will qualify
        - It will not be a cheap solution

Delivered by evolve north

- **Take a step back**
  - Based upon current and past experience
    - Business needs/user expectations
      - Rarely the same
      - Absolutely define the justification and need(both sides)
      - Define how it will be delivered
      - Risk assess, Risk assess, Risk assess
      - Get all involved (Prince 2 Project board is a good approach) include users and stakeholders
      - Get senior management to understand and accept all unmitigated risks (formally)
      - The above should create a requirements plan for Policy/Procedure, Legal, Acceptable Devices (and operating systems)Technical controls (MDM/NAC etc.)
    - BYOD (additional)
      - Define cost (may not be the “silver bullet”)
      - More risk assessment – never enough risk assessment!
      - Be absolutely brutal in the business benefit analysis
      - Make sure users understand just what they are signing up to

Delivered by evolve north

- **Take a step back (continued)**
  - 80/20 (the oldest cliché in business)
    - Key things IG/IT need to do
      - Take control (lead this thing)
      - Get all involved
      - Be positive
      - Risk assess
      - Ensure pilot projects are run (and monitored)
    - We can't be the Luddites
      - Mobile and remote is here don't ignore it or assume existing approaches meet the need
      - BYOD is coming – but it must be on our IG/IT terms
      - BAD (Bring Any Device) is not going to happen – we can't allow it
      - Embrace it!

Delivered by evolve north

- **The six steps**

1. Admittance
   a) Accepting you have to deal with and manage the issue
   b) Acceptance of the above by all in the business
2. Understanding
   a) Execute a gap analysis (ISO27001 appendix A)
   b) Risk assess gap analysis outputs
3. Remediate
   a) Create a plan to fix the issues
   b) The plan must be realistic (use gap analysis and risk assessment's to set priority)
4. Deliver
   a) Manage delivery as you would any project (Prince 2?)
   b) Have a project board and demonstrate progress/issues as part of the project
5. Maintain
   a) Establish on-going audits and checks
   b) Hold regular IG meetings
6. Educate
   a) At all levels
   b) As often as possible

Delivered by evolve north

- **Take a step back (continued)**
  - One last thought
    - CIA (Confidentiality, Integrity and Availability)
      - The corner stones of Governance
        - Confidentiality (just lock it away)
        - Integrity (just lock it away)
        - Availability (the tricky bit)

Our challenge is to get the availability part right

every single time……

Delivered by evolve north

- **Questions?**

Mark Dennis

mark.dennis@evolvenorth.com
www.evolvenorth.com

07968 537115

0191 3006400