

# ISACA – Chapter Meeting

Notes from 19<sup>th</sup> May meeting

RANT

# What New Product or Solution would you like to see on the market?

- Abolish the concept of a computer file. (Too easy to duplicate data)
- A product that will convert policies into a real-time control to ensure compliance
- A different solution other than standard A/V for controlling viruses
- A monitoring solution to solve the problem of “lots of logs, but no checking”
- A product to control access across mid-range platforms
- A products that matches compliance requirements against encryption standards.

# What is the biggest topic keeping you or your CISO awake?

- Control of data through privileged access
- Privacy
- Changing threat-scape
- Export controls
- Meeting regulatory requirements
- Employee data
- Compliance with contractual data handling requirements
- How to convey the “right” risks to senior management
- Management assess/embrace idea of risk, but not consistent with what actually happens
- People are fallible
- Secure email that is seamless
- Virus protection (McAfee product)
- How to get people to be proactive about security and not reactive

# General Gripe...

- Are IT suppliers ignoring the new and emerging threats to the netcentric organisation and protecting established brands and revenue streams?
  - Will new protective technologies arrive once there is an established demand, and what happens to your business in the mean time?
  - As IT leaders what can we do to limit our business risk?
- Keeping CPEs
- Access to social network sites
  - Attitude of marketing
  - “Business need” (perceived)

# General Gripe...

- Consolidation needed
- Supplier pitches are too “random” with respect to prices
- Government can’t share protectively marked documents across appropriate audience
- People do not understand the value of data
- People don’t understand risk
- Microsoft is full of bugs
- Lack of money to invest in security

# Discussion time #1

- On Risk in general
  - The difficulty is getting people to understand risk. (Reference was made to an article on risk perception by the Royal Society)
  - Some risks are impossible to quantify. E.g., what is the risk that there will be a zero-day vulnerability tomorrow.
  - Need to start to bring people back to their business and ask what risks they should address first
  - The way people perceive risk is important
  - We are good at perceiving near-term and personal risk, but bad at other.
  - Directors often have no understanding of the risk, because they can get another job!
  - The first time that someone (e.g., director) gets fined, will make risk “Personal” again.

# Discussion time #2

- Need a product that will convert policies into a real-time control
  - Such a product may exist. Look at Avertus – Vigilante Pro.
    - So long as you have initial data classified then it will enforce policies.
  - Some products will lock your PC as you walk away from your desk.
  - HP provide their ESF solution. (eTrust Policy Compliance). Can support 35% - 40% of ISO27001 policy expectations

# Discussion time #3

- A possible solution to the A/V problem.
  - Take a look at the Jericho Forum. Individual devices look after themselves, but maybe a bit far fetched.
  - Compliance teams need to look at the device hardening rules.
    - Rarely find proactive approach to device hardening
    - When one exists, there is an exception policy
  - Look at Qualys – technical security standards.
- Need to have better management of exception policies.
  - Ensure there is a clear process in place covering:
    - What policy is being contravened?
    - What is the business need?
    - What is the risk?
  - Too easy to bypass, so should have top-level sign-off

# Discussion time #4

- One member raised awareness of a security device
  - USB Key that is a self-contained remote access device
    - Contains Citrix Remote Desktop
    - Biometric access
    - 2 GB of storage
    - Can be plugged into any laptop to provide secure remote access back to a corporate network

# Suggestions for future meetings

- Something on Jericho Forum
  - Can we get Adrian Secombe or Paul Simmonds along?
- Meeting regulatory Requirements
- Keeping CPEs
- Session on Risk
  - Possibly Ian Glover (Insight Consultant)
  - Look at a book called “Risk” by Dan Gardner