Cyber security

Audit NZ Update

Jonathon Berry

Consulting Partner

www.InPhySec.co.nz

What needs to be protected and/or kept available?

What assurance do I have that my controls will do that?

Notes from the field (Darwinism)

- Poor awareness and/or training
- Poor classification / valuation practices across C, I, & A
- Poor threat/risk assessments & non-compliance
- Non-business owners (CIO *et al*) accepting risks on behalf of the business
- Vulnerabilities not managed
- Controls not effective / not monitored
- Inadequate incident response – reputational damage

INPHYSEC

INTELLIGENCE . PROTECTION . SECURITY

What to do?

- Value your assets and protect accordingly – risk management
- The business owns risks, IT manages controls
- Make staff aware of:
  - what's important
  - what to do and
  - What not to do…..
- Layer controls, segregate assets
- Remove, reduce or compensate for vulnerabilities
- Monitor and react
- Back-up, securely
- Verify and audit

InPhySec

INTELLIGENCE . PROTECTION . SECURITY

Questions?

Jonathon Berry

Consulting Partner

www.InPhySec.co.nz