

## **CNS Security Chapter 22.4.2010 Agenda**

---

- **Dr Neil Kettle, Convergent**
  - **Good Intentions, Bad Ideas**
- **Jill Savager, FSA**
  - **IT & Data Security and the FSA**
- **Kevin Dowd, Convergent**
  - **Compliance, Risk & Life on Other Planets**



## AGENDA

---

- **Responding to Compliance Challenges**

- Internal & External
- Regulatory, Commercial

- **Risk Assessment**

- Knowing the threats
- Calculating probabilities
- Calculating impact

- **Controls**

- If only someone had written a list of controls!
- Oh, they have.... ISO 27001 et al

- **Maintenance**

- Write once, read many (most compliance should be a reporting challenge)
- Continual improvement
- Continual Reassessment



## Responding To Compliance Challenges

---

- **Compliance**

- Traditionally seen as an overhead
- There to protect us from ourselves?
- Clear baseline for us to work to?
- Ideal world – compliance should just be demonstrating what you already do (!)

- **Current Demands**

- PCI DSS, Basle II, Sox, ISO 27001, FSA requirements, FISAP etc etc
- Perfectly possible for > 10 compliance regimes to have an impact on IT Security
- External pressures – inc customers!
  
- All of these have something in common, however...



## RISK ASSESSMENT

---

### • Threats

- An under-examined area of risk assessment
- Consider threat sources, threat actors
  - Journalists? Insiders? Competitors?
- Consider attack vectors
- Continually re-examine
- Stay close to external news sources
- Incident Reporting!!



## RISK ASSESSMENT

---

### • Probabilities

- Assessing probability is not easy!
- E.g. Drake Equation (with thanks to Paul Davies). N is the number of civilisations in the galaxy we are capable of detecting (radio emitting)

$$N = R^* f_p n_e f_l f_i f_c L$$

- $R^*$  = rate of formation of sun-like stars in galaxy (known)
  - $f_p$  = fraction of stars that have planets (capable of estimation)
  - $n_e$  = number of earth like planets (capable of estimation)
  - $f_l$  = **number of earth like planets where life occurs (varies between 0 and 1 – therefore effectively unknown)**
  - $f_i$  = **fraction of planets where intelligence emerges (no idea)**
  - $f_c$  = fraction of planets on which technological civilisation emerges (?!)
  - $L$  = lifetime of such a civilization (your guess is as good as mine)
- **Lesson** – sometimes its hard to assess probability, particularly with a small sample size! As the dataset increases, the above will unravel
  - **BUT, it can help to unpack the equation a bit (e.g. virus outbreak)**

## RISK ASSESSMENT

---

- **Impact**

- Financial impact can be difficult to quantify
- However, can look at the elements:
  - Cost to fix
  - Fines
  - Re-work cost
  - Opportunity cost
  - Lost business
- **BE REALISTIC**
  - Would the work have been done another day?
  - Look for real life incident patterns – can you correlate vs actual costs or business results in the past?
- With all the above calculations, don't be afraid to quantify your uncertainty
- E.g. might calculate a risk and provide a number, but qualify with the fact that the result is uncertain, and highlight the data required



## CONTROLS

---

- **ISO27001**
  - Best practice exists and can be referred to!
  - Not complete, but a good baseline
  - Good for process and goals and baseline controls
  
- **More Specific Technical Controls**
  - PCI DSS
  - SANS, CIS etc
  - Vendors (with a pinch of salt)
  
- **Control Effectiveness Assessment**
  - Very, very difficult
  - Make use of information sources
  - Invest in detective capability
  - Continual assessment



## **MAINTENANCE**

---

- **Write Once, Read Many**
- **Continual Improvement?**
- **Continual Assessment**

