

SECURITY CHAPTER

January 2010 Briefing



Next Briefing

April 22nd 2010

Jill Savage – IT & Data Security – **FSA**

.FSA Handbook and other industry standards

- . * What is Arrow?
- * “More intrusive supervision”
- * IT Risk Management (as a subset of Operational Risk Management)

June 2010 – You tell us.



AGENDA

- **General Survey of what CNS see in the marketplace**
 - Meandering, but hopefully meaningful **(and only 12 slides)**

- **Background**
 - Regulation, Legislation

- **Threats**
 - New threats, and some old favourites

- **Incidents**
 - Time to face the fact that incidents happen all the time...
 - ... but they don't cost an average of \$1bn per incident
 - Incident types
 - Building a corporate memory for incidents

- **Challenges**
 - Technical Challenges
 - Operational Challenges



AGENDA

- **Spending Focus**

- There is no standard spending focus
- There is no standard amount of money spent...
- ... but we all spend too little
- And there are some themes.



BACKGROUND

- **Infosec (particularly IT Security) has not had a higher profile than it has at the moment**
- **WHY?**
 - Regulation (are you the only house without an alarm?)
 - Legislation
 - Customer Demands
 - Incidents, incidents, incidents...
 - Generally a larger Infosec focussed ecosystem



BACKGROUND

- **IT has never hidden underlying complexity of systems more so than it does now**
 - Reduced understanding
 - Easier deployment – poorer understanding of the issues
 - Customers demand fast deployment...
 - ... IT don't have the time or knowledge to get security right



THREATS

- **Same old, same old**
 - Malware merry-go-round, still some defacements
- **Organised Crime & Government Sponsored Hacking**
 - Money to be made
 - Increased organisation and efficiency
 - Leads to...



INCIDENTS

- **Quiet Incidents..**
 - Quiet malware
 - Major change in focus for black hats
- **& Targeted Attacks**
 - Particularly against Senior Company Officers
 - Otherwise known as the exceptions...
- **Blue on Blue Incidents**
 - ID Theft
 - Theft of Financial Details
 - Whole new dimension to consider
- **Data Leakage/Data Ransom**
- **Internet Explorer**
 - AKA the current greatest threat to your network?



CHALLENGES

- **There's a lot going on...**
- **Operational Resource**
 - IT Security's biggest challenge, bar none
 - Org Charts don't help. Imagine an IT Security Manager tasked with meeting threats to Web Application Security:
- Scenario 1 – IT Security Manager is also the Network Manager. He buys an application firewall.
- Scenario 2 – IT Security Manager used to to be the Network Manager and only Networks will talk to him (or have resource). He buys an application firewall
- Scenario 3 – IT Security Manager has remit across the organisation. Web Development talk to him, but don't have anyone to do the work. He buys an application firewall.

CHALLENGES

- **Patching**
 - Still many not patching OS
 - Very few are patching apps
 - Effective approaches are part auto, part manual with VM based testing
- **Effective AV**
 - Is AV now the biggest user of CPU cycles on corporate networks?
 - Zero Day
- **Data Marking**
 - Few have identified data assets and owners
 - Data risk poorly understood
 - Size of the task puts most people off
- **Understanding ACTUAL Risk**
 - See previous comment on Corporate Memory
 - No “actuarial” tables (so build some!)
 - Threat modelling rarely undertaken
 - Hampers communication with the business
 - How can you plan spend without knowing the risks?

SPENDING FOCUS

- **Traditional Areas still strong**
 - Firewall
 - AV
 - Proxy/Content Filtering
- **Data Leakage Prevention**
 - Which is what, exactly?
- **Monitoring & Logging**
 - Most people have no way of tracking or being aware of incidents
 - And no forensic capability
- **Identity Management**
 - Still a huge issue
 - No consistent trends
- **Compliance Costs**
 - Surprisingly immature
 - Most organisations are still getting this right, rather than being cost effective



SANS Top 20

Client Side Vulnerabilities

- C1. Web Browsers - **Some spend, sector dependent**
- C2. Office Software - **Often neglected**
- C3. Email Clients - **Some spend, sector dependent**
- C4. Media Players - **Often neglected**

Server Side Vulnerabilities

- S1. Web Apps - **Generally well supported (although code less so)**
- S2. Windows Services - **Patching generally bad**
- S3. Unix and Mac OS Services - **Some spend, sector dependent**
- S4. Backup Software - **Often neglected**
- S5. A/V - **Generally well supported**
- S6. Management Servers - **Generally well supported**
- S7. Database Software - **Often neglected**

SANS Top 20

Security Policy & Personnel

H1. Excessive User Rights and Unauthorised Devices - **Some spend, sector dependent (changed)**

H2. Phishing/Spear Phishing- **Often neglected**

H3. Unencrypted Laptops & Removable Media - **Some spend, sector dependent (changed)**

Application Abuse

A1. Instant Messaging - **Often neglected**

A2. Peer to Peer - **Often neglected**

Network Devices

N1. VOIP Servers & Phones - **Often neglected**

Zero Day Attacks

Z1. Zero Day Attacks - **Often neglected**

TRADITIONAL FOCI DOMINATE; VERY LITTLE CHANGE; LOTS OF HOLES

WHAT WOULD WE DO?

- **Regular Controls Review**
 - Control effectiveness and coverage
 - Challenge in full on a 3-5 year rolling basis
- **Understand Business Threats and Risks**
 - Scenario Modelling
 - Corporate Memory
- **Spend Money on People**
 - Operational Resource
 - Awareness & Training (See DLP above...)
- **Some of the Areas on the previous slide...**
 - Traditional areas (FW etc)
 - Monitoring & Logging (hugely important and rarely done)
 - ID Management – still the easiest way in for our testing team
- **Questions?**