

“Ground Zero” Case 2002

Dave Tyson, MBA, CPP, CISSP
Manager, IT Security
City of Vancouver

April 3, 2003

Agenda

- Review of case details
- Organization’s reaction
- Consultant Approach
- Results
- A little Real world Information from today on the challenges for security



Case Background

- BC Organization – Part of a North America Wide organization
- 725,000 customers province wide
- They were hacked and loss sensitive data, although what was lost was not well understood
- The Parent organization threatened them with sanctions should they not resolve their security issues fully and quickly



Organization’s Reaction

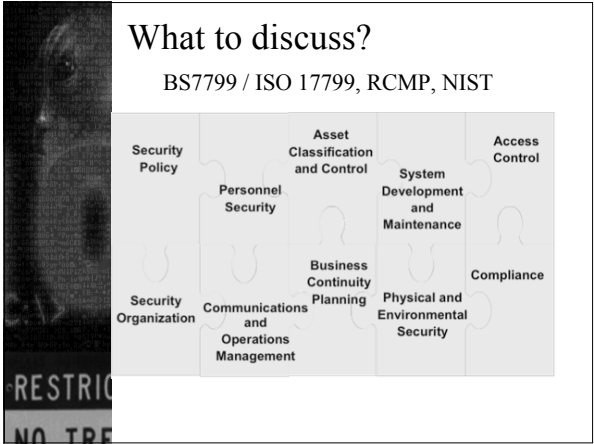
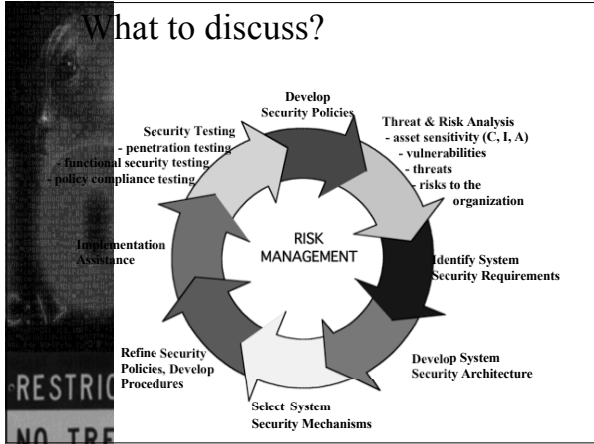
- Panic!
- Yelling!
- Finger pointing!
- The search for the guilty!
- Then,they called IBM

Situation Summary

- Organization with no formal security program and undefined risks
- Castle mentality – perimeter firewall and SSL makes me secure
- No dedicated security resources or defined accountability
- No plan and clear understanding of the level of risk present – lots of undefined expectations

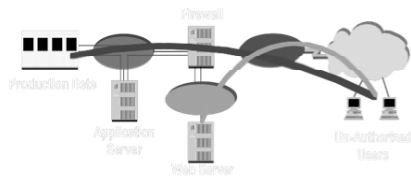
Consultant's Approach

- Introductory seminar and interviews
- TRA
- Security review against measurable standard
- Gap Analysis
- Recommendations with quick wins
- Debrief at all levels
- Implementation assistance



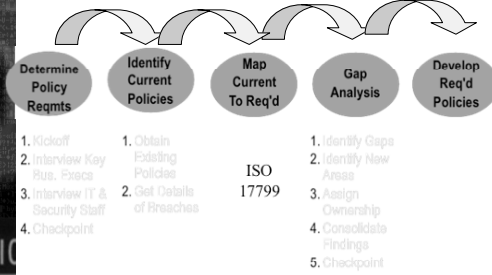
What to discuss?

Segmentation



What to discuss?

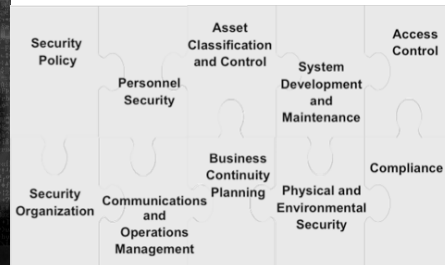
Policy & Standards Dev.




Threat & Risk Assessment

- Define a TRA methodology to be used – must know how much information is available and what the tolerance of the organization is for quantitative results – No one way to do it!
- Multi disciplinary group for qualitative assessment component
- Includes internal and external pen tests


Security Review Against a Measurable Standard






Gap Analysis

- Should relate back to organization strategic plans or initiatives
- Some sensitivity to industry or market
- Language speaks to all levels of organization




Recommendations

- Quick Wins
- Order in criticality
- Specific technology fixes required
- Build a strategic plan for 1-5 years in platform agnostic terms




Debrief

- Presentations tailored for multiple levels – with similar messages
 - Senior Mgt.
 - Line Staff
 - Technical




Implementation Assistance

- Time
- Resources
- Criticality of issues




The Result

- 3 year plan
- Last external pen test received top marks – no external penetrations
- Internal policy violations are down by 80% over the last year




A little real world info

- 80% of e-mails we get are malicious or spam
- 24000+ virus e-mails per week
- Every computer I have reviewed has had Spyware on it
- 80% of your time should be spent on the human issues – 20% pure technical issues



Questions?



Thank You

Dave Tyson, MBA, CPP, CISSP
Manager, IT Security
City of Vancouver
dave_tyson@city.vancouver.bc.ca