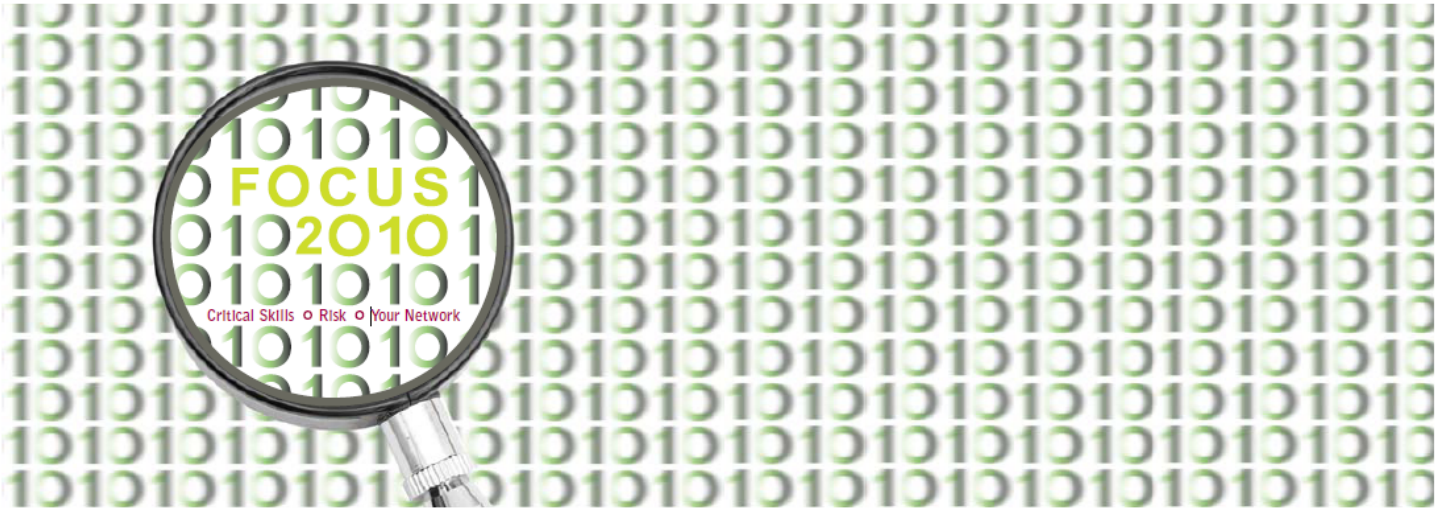
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



G13: Is Network Security Dead or Obsolete?

Eddie Borrero, Robert Half International

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Is Network Security Dead or Obsolete?

Learning to sell network security projects to upper management

Questions I get asked as CISO…

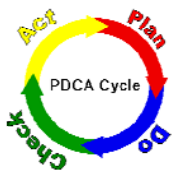
Question	Typical - Risk Mitigation
Do you know where all of your sensitive data is stored and who has access to it?	Data Classification Content and IP Protection
Do you outsource data processing to third parties? If so, how do you get comfort that they are taking appropriate measures to protect your sensitive data ?	ISO27001 review
Would you be aware if a security incident occurred and be able to quickly react to it?	Security Incident Response – Security Event Management - Content Monitoring and Filtering
Does your security group feel that they spend more time preparing for audits and being reactive than moving forwards strategically? How much of securities time is responding to incidents rather than proactive?	"Getting ahead of the audit curve" ISO 27001 Review
Are you aware of significant inconsistencies between policy and practice?	Policy and Procedure development ISO 27001 review
Are you able to provide a current picture of regulatory compliance and gaps (GLBA / HIPAA / SOX etc)? Are you addressing GLBA, HIPAA etc with point solutions?	Regulatory Compliance / Framework project
Are you able to show your board metrics on how security is performing (and whether enough / too much money is being spent?)	Balanced Score Card
Do you have controls over the security of end-user devices such as laptops / PDA's etc?	End-to-end device security (incorporating IT asset management elements)
Would a request from one of your customers / partners related to security result in a 'fire drill'?	Security Incident Response – Security certification

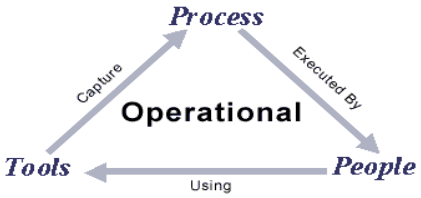
ISACA
San Francisco Chapter

Common Security Risk Management Processes Presented to Me

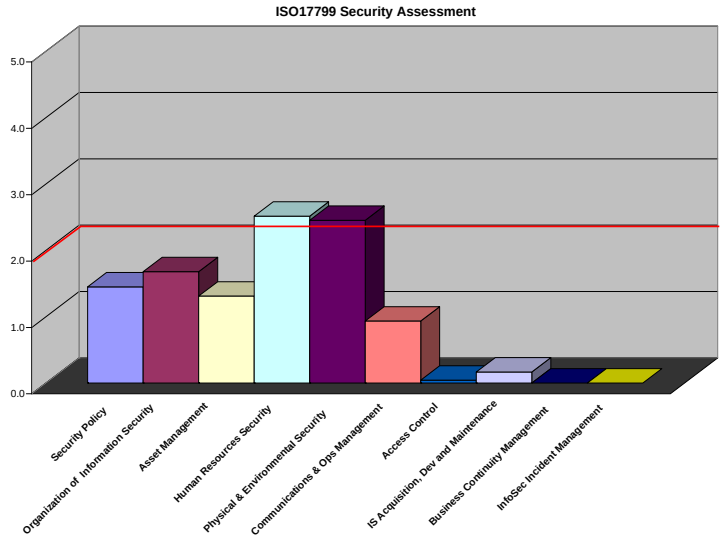
- User management
- Vulnerability management
- Patch management
- Compliance and enforcement
- Risk management
- Incident management
- Investigations
- Business continuity planning

- Data Leakage Prevention / Rights Management
- Awareness
- Metrics and reporting
- Software Development lifecycle
- 3rd party vendor management
- Logging and alerting
- Policy development and rollout





Sample Graph of Security Assessment



- If these are the types of things being discussed at the executive level how do we tie network security initiatives back to things our business cares about?

Here's the methodology we use!

For every project we put it in the context of the following guiding principles:

- Cost Savings – will this effort save us time and or money as a company?
- Business Enablement – will this effort enhance our employee and or customer experience / productivity?
- Risk Management – will this effort reduce a security or compliance risk for the organization?

Lets Run a Simulation to see how this works

- Get folks into a 3 groups and give them a scenario where they will need to ask for funding for :

- NAC at a global company…
- New Firewalls
- IPS