

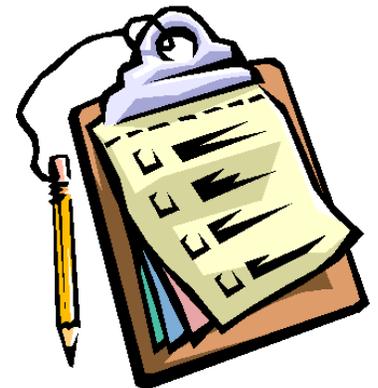


Future Trends: Why your Security program has to change going forward

Manny Morales
CISSP, CISA, CISM, CSM
Independent Consultant
June 2, 2015

The Topics

- ▶ Issues
 - Data Breaches
 - Why we still have them
 - Defense in Depth
 - Poor Risk Management
- ▶ Solutions
 - Breach Laws
 - Frameworks
 - Risk Management
 - Partnerships and Governance



Issues



What are the issues

- ▶ Unauthorized Access
 - Deliberately- the Hackers
 - Depended on others to protect – third parties
 - Risk takers – not understanding the data
 - Accidental – bad installation
 - Weak skill set of IT implementers
- ▶ Authorized Access
 - Separation of Duties
 - Bribery or Corruption
 - Retribution



Data Breaches

- ▶ Target – Payment Card System (40M)
- ▶ Home Depot – Payment Card System (56M)
- ▶ TJ Max – Wireless attack
- ▶ Sony – Email
- ▶ Anthem – Data breach (80M)
- ▶ South Carolina Government – Tax Records
- ▶ Texas Comptroller – Server Breach
- ▶ Federal Government – They don't know



How do Data Breaches happen

- ▶ Inadequate Patching
- ▶ Email malware and Social Engineering
- ▶ The use of third parties
- ▶ Unmonitored remote access
- ▶ Not using encryption
- ▶ Not enough separation of duties
- ▶ No testing of controls
- ▶ Depending on IT alone
- ▶ Weak skill sets of personnel



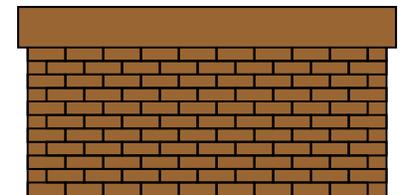
Why do we still have issues

- ▶ Entities view Cyber Security as an IT issue
 - IT views security as a afterthought
- ▶ Risk out-weight the breach cost – but that is changing
- ▶ Foreign Governments want information
- ▶ Very little cooperation within other entities
- ▶ Sharing data makes money for companies
- ▶ Not working with Business leaders



Defense in Depth issues

- ▶ Dependence on Firewalls and Proxies alone
- ▶ Use of security tools only – where the money is spent
 - Limited security skill sets
- ▶ Not allowing new technologies to integrate
- ▶ What management wants, trying to create the magic ‘Black Box’
- ▶ Weak monitoring
- ▶ No focus on recovery

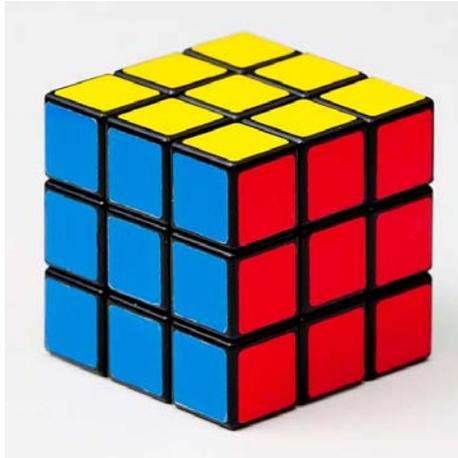


Poor Risk Management

- ▶ It is an Internal Controls requirement, however it is a paper process
- ▶ Too much ‘the sky if falling’ attitude
- ▶ No entity wants to air their issues
- ▶ Its too self managed
- ▶ Very little follow-ups

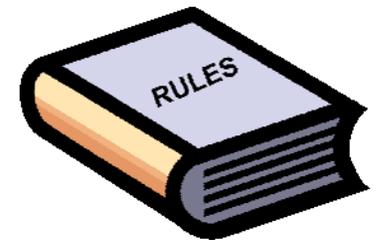


Solutions



Data Breach Laws

- ▶ Not every state has a law – 47 states have – SD, NM, AI don't have one
 - Some laws also protect Health Care information
 - Some are requiring security programs
 - Some are for electronic data alone
- ▶ New Federal law overrides state laws – however it could weaken some state laws
- ▶ EU is enacting new laws to protect people's rights – requiring more disclosure of where their data is stored



Why are Security Frameworks needed

- ▶ They provide the architecture
- ▶ The road map to a better security process
- ▶ Give data a Lifecycle, creation to destruction
- ▶ Some of the more established standards:
 - NIST – Fairly new
 - Cobit – More risk based
 - ISO – The Information Security standard
 - SANS 20 Critical controls – More IT focus



Security Framework

- ▶ Whatever framework is used, it must do the following:
 - Identify the asset
 - Classify the asset
 - Protect the asset
 - Monitor the asset
 - Respond to attacks of the asset
 - Be able to recover the asset
 - Properly discard the asset



NIST Framework

- ▶ Identify
 - Data Classification
- ▶ Protect
 - Access Controls
- ▶ Detect
 - Monitoring
- ▶ Respond
 - Incident Response
- ▶ Recover
 - Business Continuity



Why Security needs to be viewed as a Business

- ▶ It is the business that wants to use the Internet
- ▶ Business owns the data
- ▶ Applications are business driven
- ▶ Privacy and Security are becoming business issues
- ▶ IT is just an enabler and the cost of doing business – they don't have much say
- ▶ Its all about addressing risks



Risk Management

- ▶ Don't allow entities to do it alone
- ▶ Work with management to explain to them it is in their best interest to report risks
- ▶ Understand that business will take risks
- ▶ Not everything is high risk
- ▶ If a business takes a bad risk it can cost them '10' fold- legal, reputation, fines
- ▶ Have a workable process



Partnerships

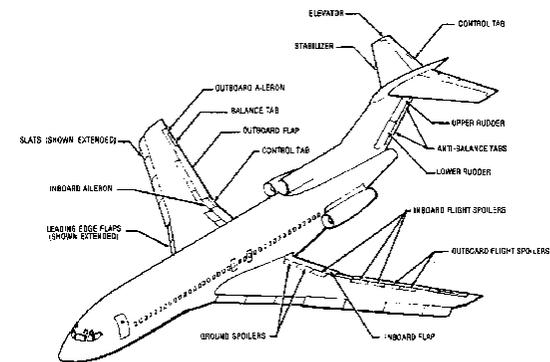


Information
Security
Officer

Privacy Officer



Internal Controls



Why Partnerships

- ▶ Security is viewed as an impediment
- ▶ Strength in numbers
- ▶ Privacy, Security, and Internal Controls have common objectives
- ▶ Don't forget to associate with Business entities



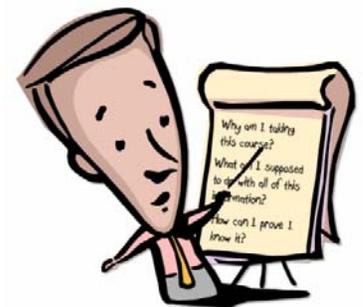
Cyber Security Governance

- ▶ It elevates security to a management process
- ▶ Members should be business reps, CIO, ISO
 - Makes the rules
 - Reviews the policies
 - Acts on a breach
 - Request status of security
 - Address risks
 - Funds cyber security program and staff
- ▶ Tie-ins with the entity goals



In Summary

- ▶ There will always be risks
- ▶ There will be a breach at sometime
- ▶ Need to Partner
- ▶ Need to engage Management
- ▶ Use other experts as needed



Thanks

- ▶ My email is: manny_morales@hotmail.com

