Virtualisation Security for Regulated Environments

SCADA CoI, 19 May 2011

Conference Release, May 2011

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney, NSW 2000,
Australia

Melbourne
Level 8, 350 Collins Street
Melbourne, Victoria 3000,
Australia

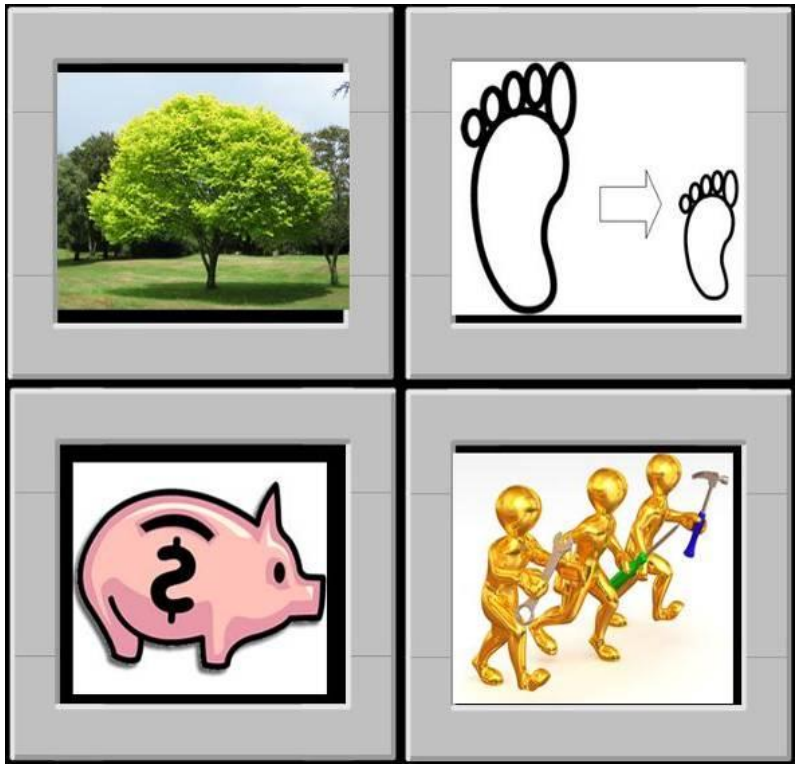
T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

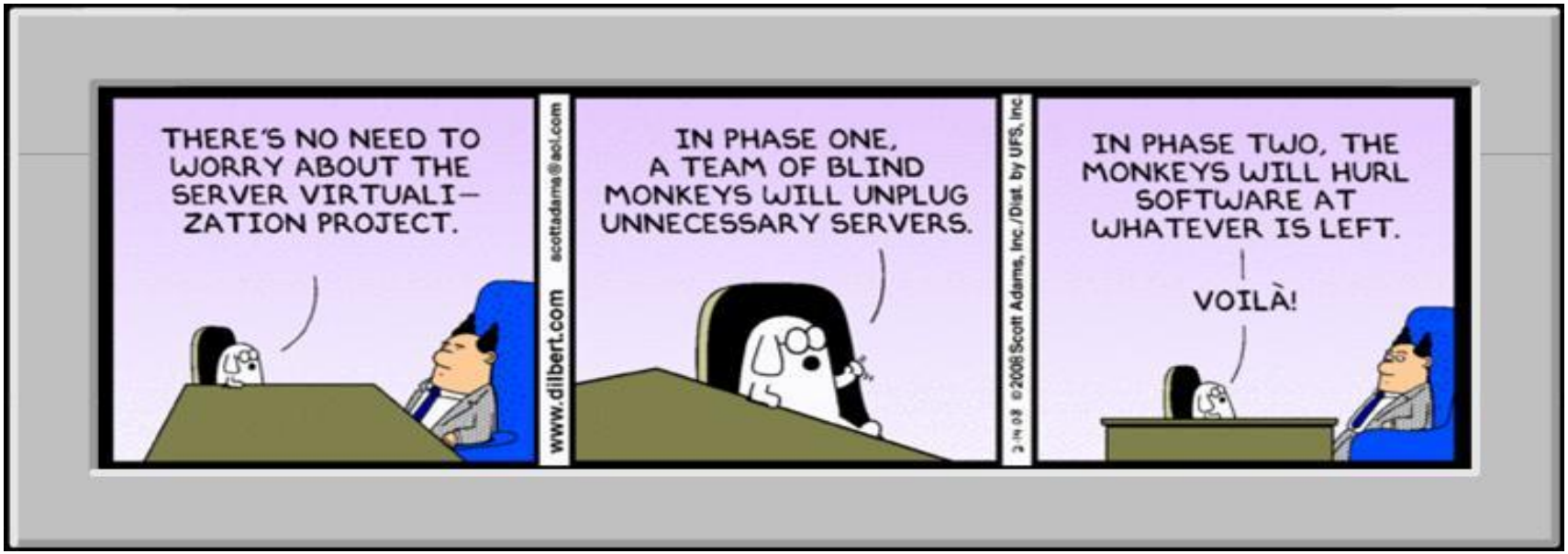
Agenda

- Introduction to Regulations
- Virtualisation Security Challenges
- Implications for Regulated Environments
- Be Prepared
- Conclusion

Virtualisation Benefits

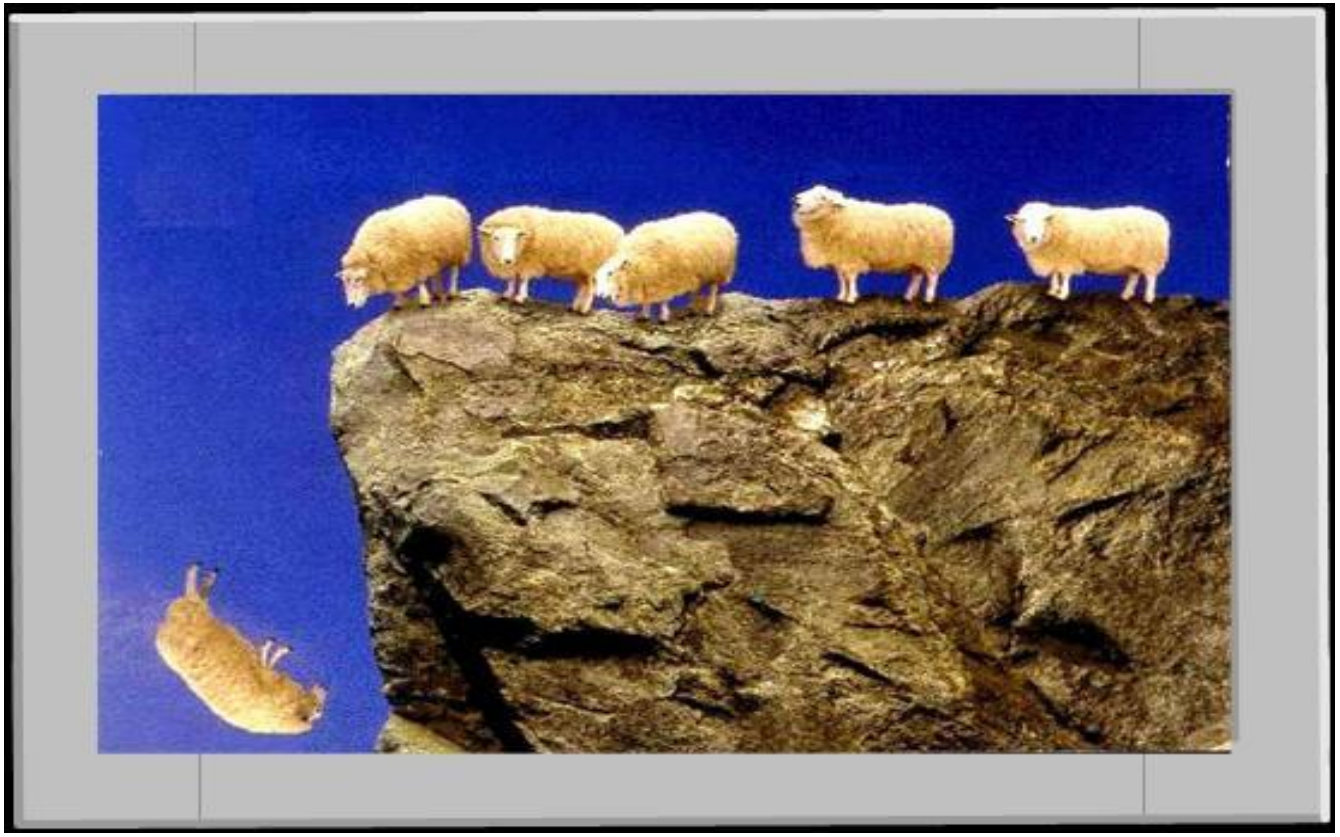


Even Dilbert's boss is onto this!



Licensed

It’s so easy, follow me



Virtualisation, Regulation & Guidance

- Australian Government
  - ISM, PSPF
- US
  - National Institute of Standards and Technology (NIST) x 2
  - NERC North American Electric Reliability Corp (NERC)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - Defense Information Systems Agency (DISA)
  - Dept of Homeland Security (DHS)
- Intl
  - International Society for Automation (ISA)
  - International Electrotechnical Commission (IEC)
- Other Guidance
  - Cloud Computing Alliance (useful mapping tools)
  - Even the payment industry PCI DSS (2.0), Virtualization Special Interest Group (Info Supp and mapping tool due soon)
  - Cloud Computing Guidance (AGD, Dept of Finance, DSD)

ANSI/ISA-99.02.01-2009

- 4.3.3.4 Element – Network Segmentation
- Objective:
  - Group and separate key IACS devices into zones with common security levels in order to manage security risks and to achieve a desired target security level.
- Requirement 4.3.3.4.1
  - A network segmentation countermeasure strategy employing zones shall be developed for IACS devices based upon the risk level of the IACS

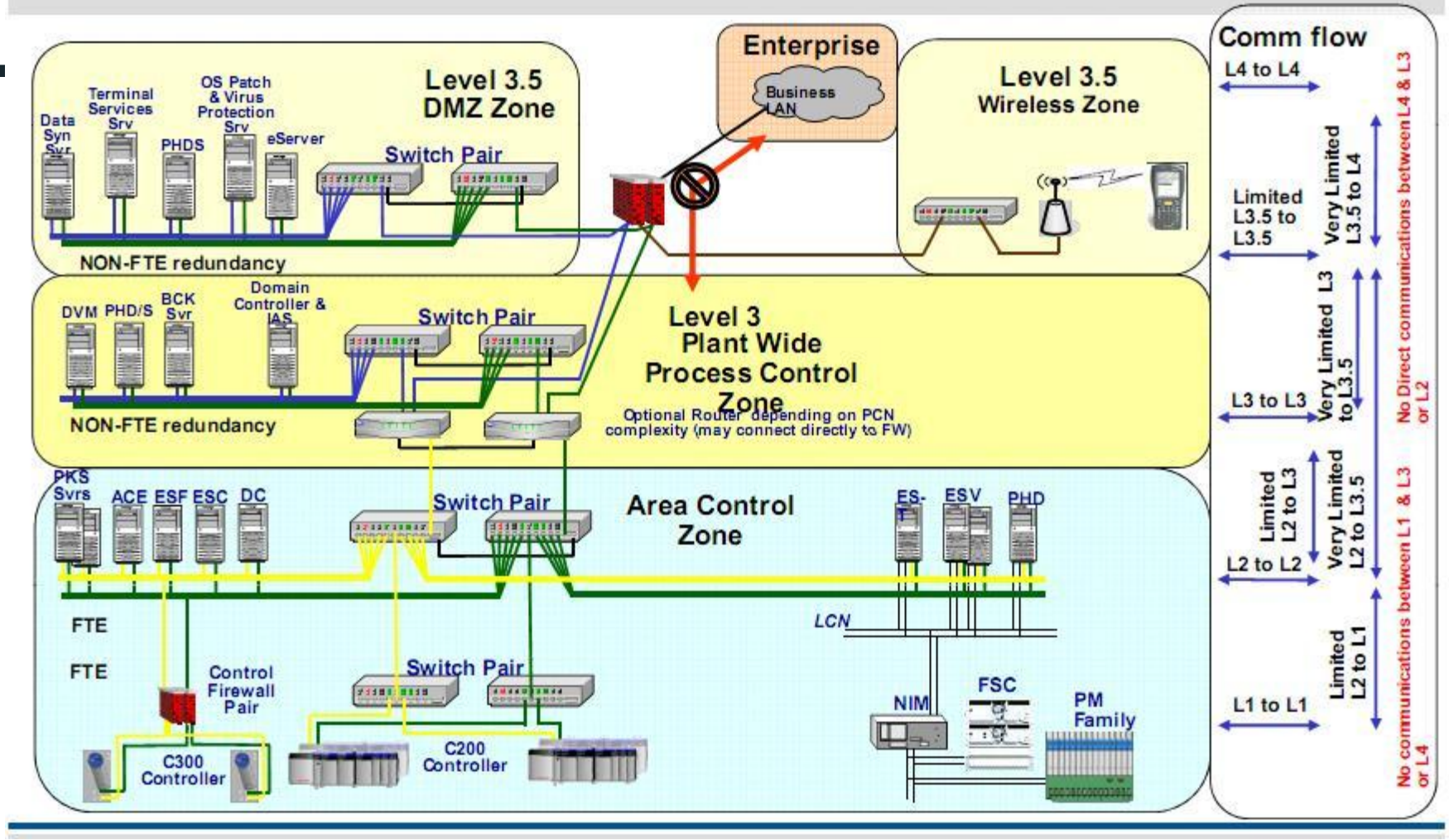
Security Zone Definition

- "Security zone: grouping of logical or physical assets that share common security requirements " [ANSI/ISA-99.00.01-2007-.2.116]
  - A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements
  - "The security policy of a zone is typically enforced by a combination of mechanisms both at the border and within the zone."
- E.g. HMI Zone and Controller Zone

Conduits

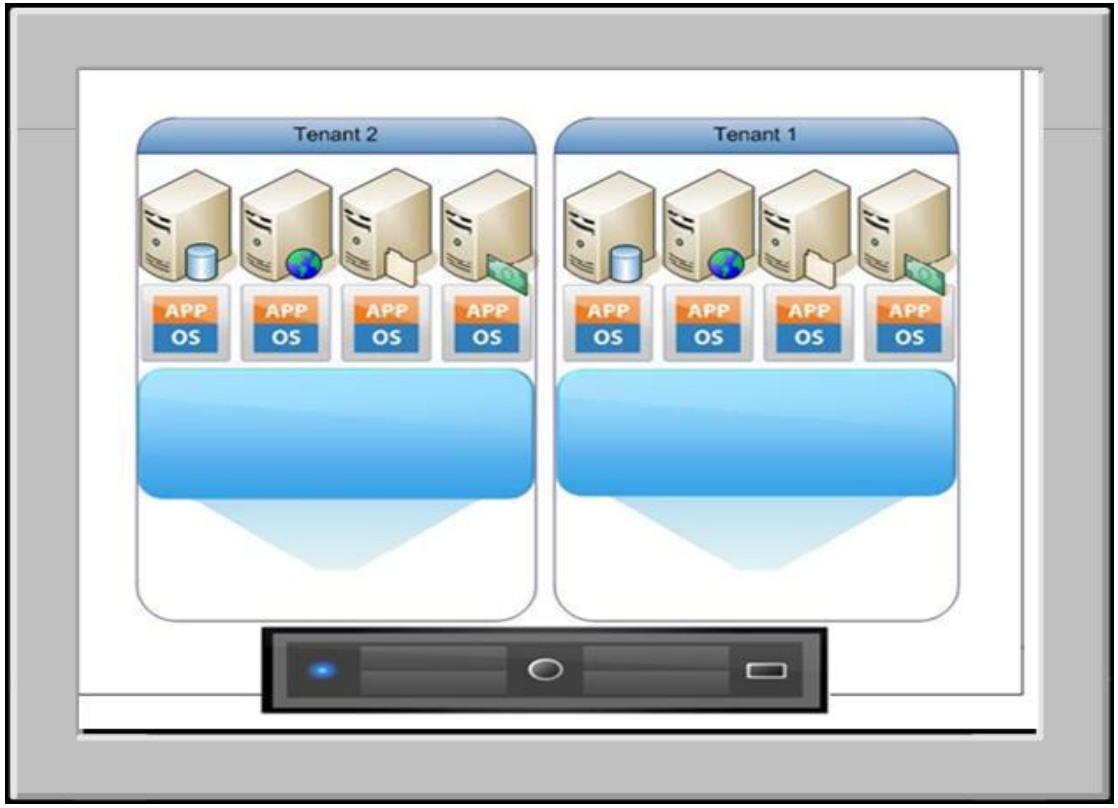
- A conduit is a path for the flow of data between two zones.
  - Can provide the security functions that allow different zones to communicate securely
  - Any communications between zone must have a conduit

Network Architecture as Zones

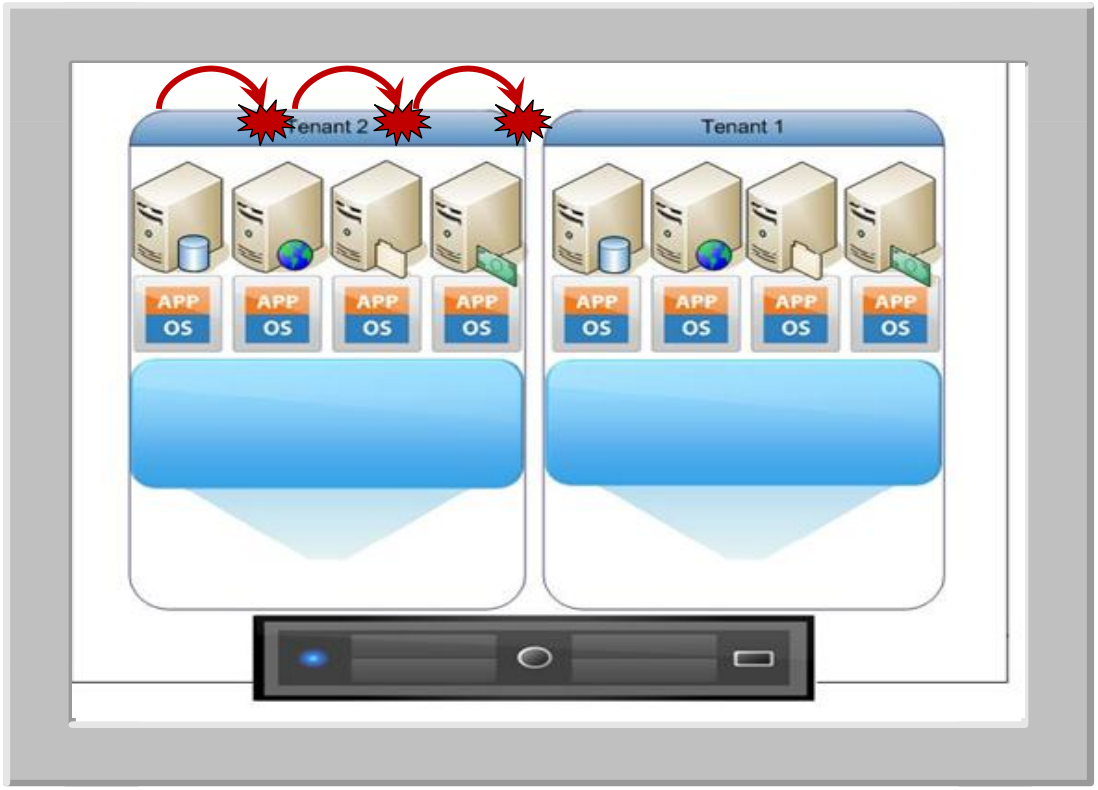


Honeywell – Securely integrating multiple systems together as an ICS

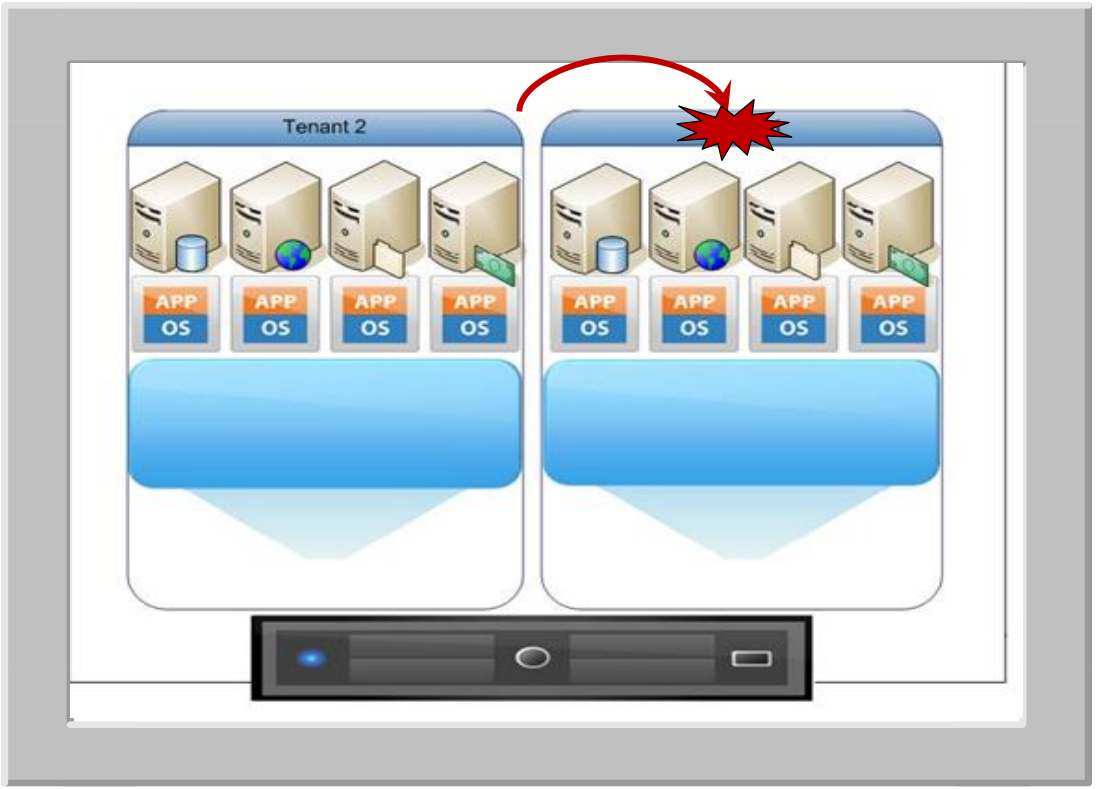
Sample Scenario - Multizone or Internal



Guest to Guest Compromise



Guest to Guest - Inter-zone Compromise

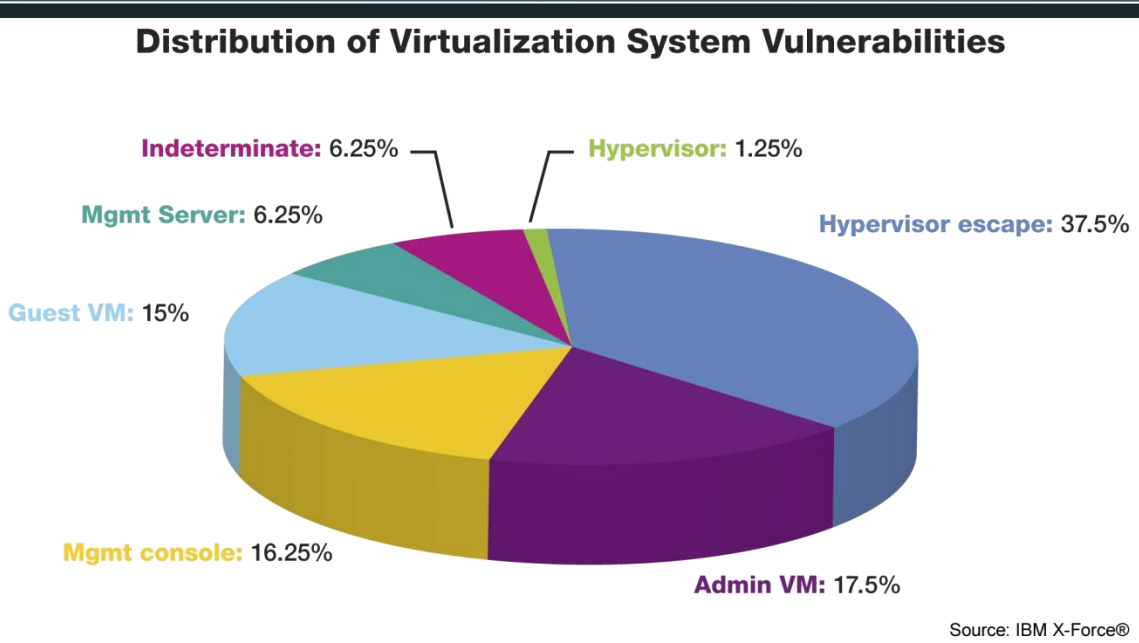


Guest to Host (HV) - Worst Case

How does it happen?

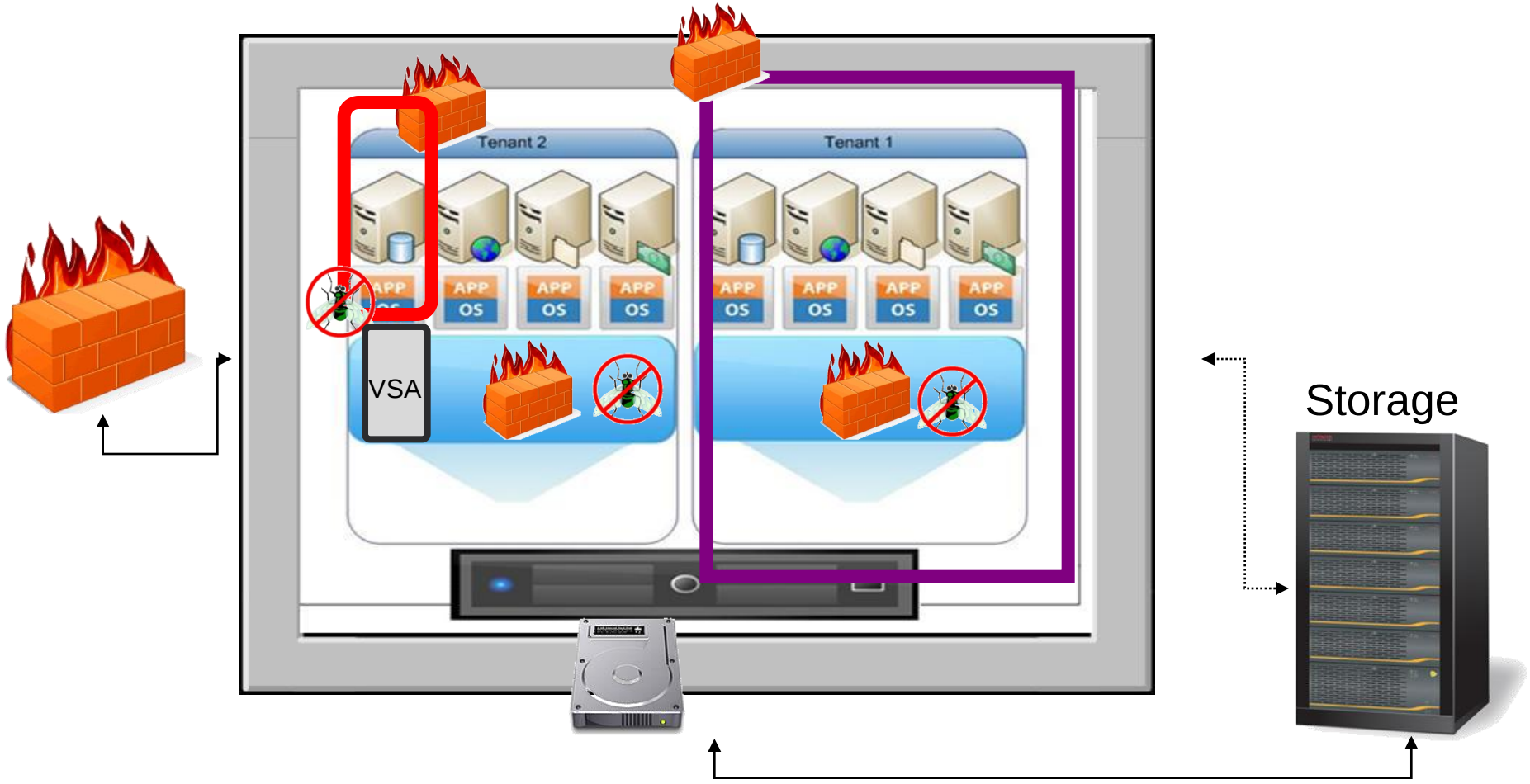
- Hypervisor should prevent guest-to-guest or guest-to-host compromise
- However, if mis-configured isolation may not be effective
  - Poor setup of virtual networking
  - Optional features such as drag-and-drop, clipboard sharing etc. may break isolation
  - No secured management VLAN
  - Hypervisor & guest itself not secured
  - Ineffective controls to protect Hypervisor & guest (patch mgt, access control, auth)
  - Root Hypervisor Vulnerability

Vulnerabilities & public exploits



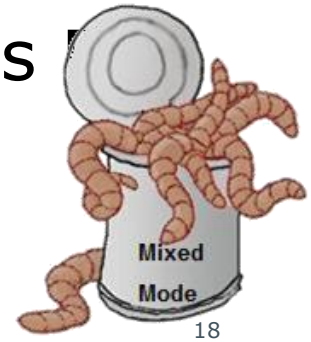
"Of particular note here are the first two classes of vulnerabilities. **The most common class of vulnerabilities in server class virtualization products, hypervisor escape vulnerabilities, generally represents the most serious risk to virtualization systems as these vulnerabilities violate the principal of isolation of virtual machines**. The next largest class of vulnerabilities, administrative VM vulnerabilities, also present serious risk, as these can provide control over the configuration of the entire virtualization system."
[IBM XForce 2010 Trends Report] [5]

Where is the protection applied?

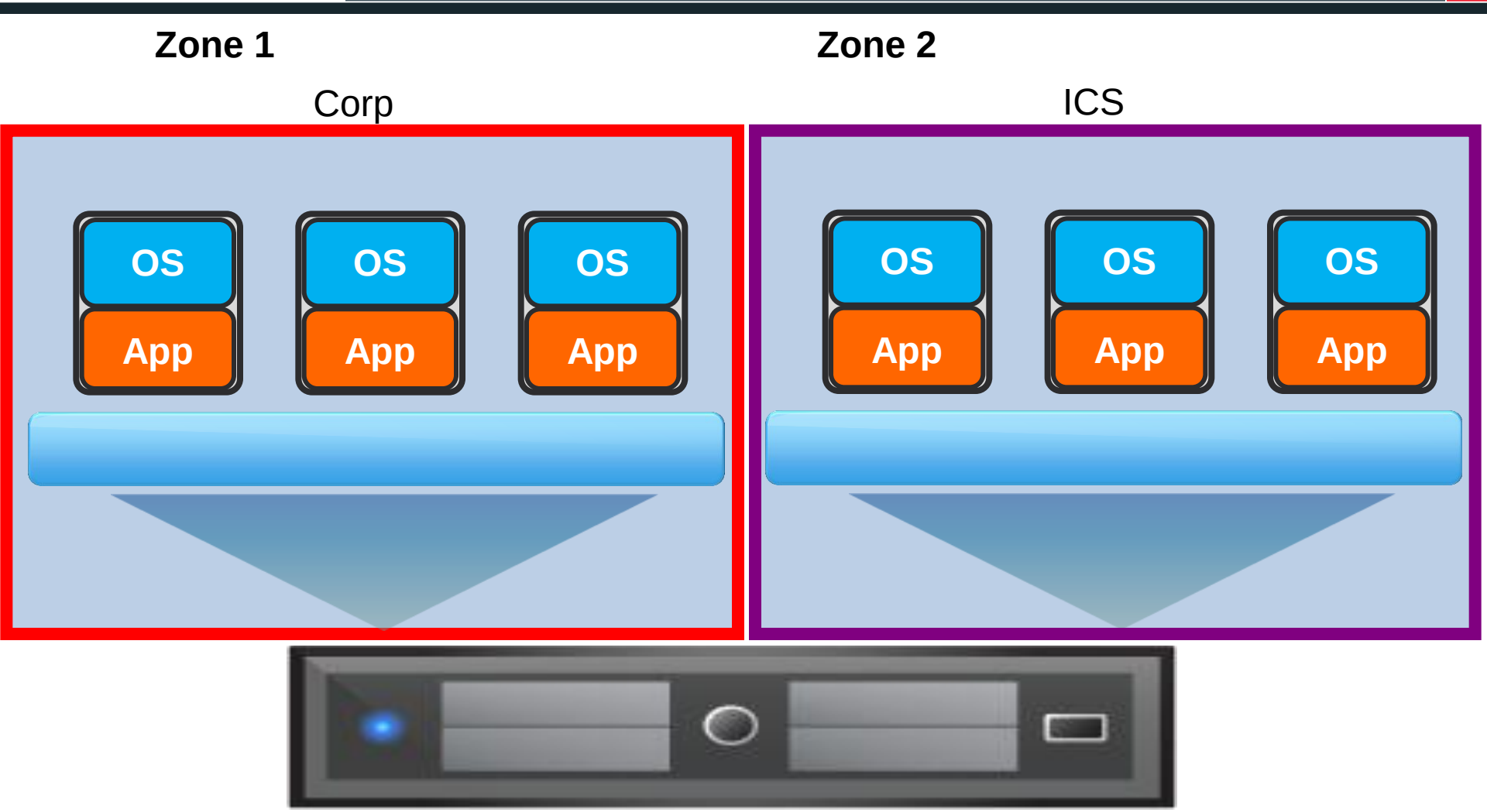


The Solution?

- Physically isolate zones of trust?
- Co-hosted but isolated? Separate Virtual Switches?
- Risk Assessment (ISM Control: 0750; PSPF Gov-6, NIST 800-82 4.2.6, PCI DSS Req 12.1.2 and defined in VSIG guidance)
- In the case of virtualised "mixed mode" implementations, the risk assessment must demonstrate the segmentation has been achieved at a level that meets or exceeds [illegible] Reqs.

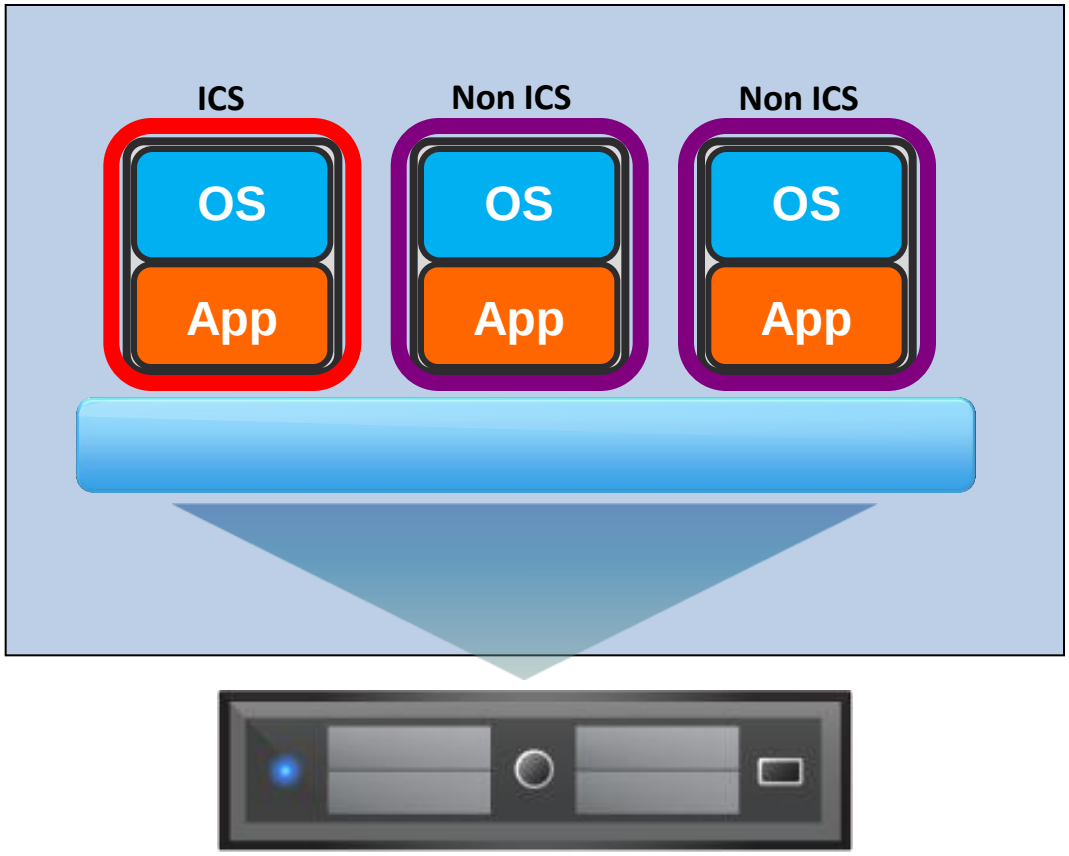


Mixed Mode - Multizone

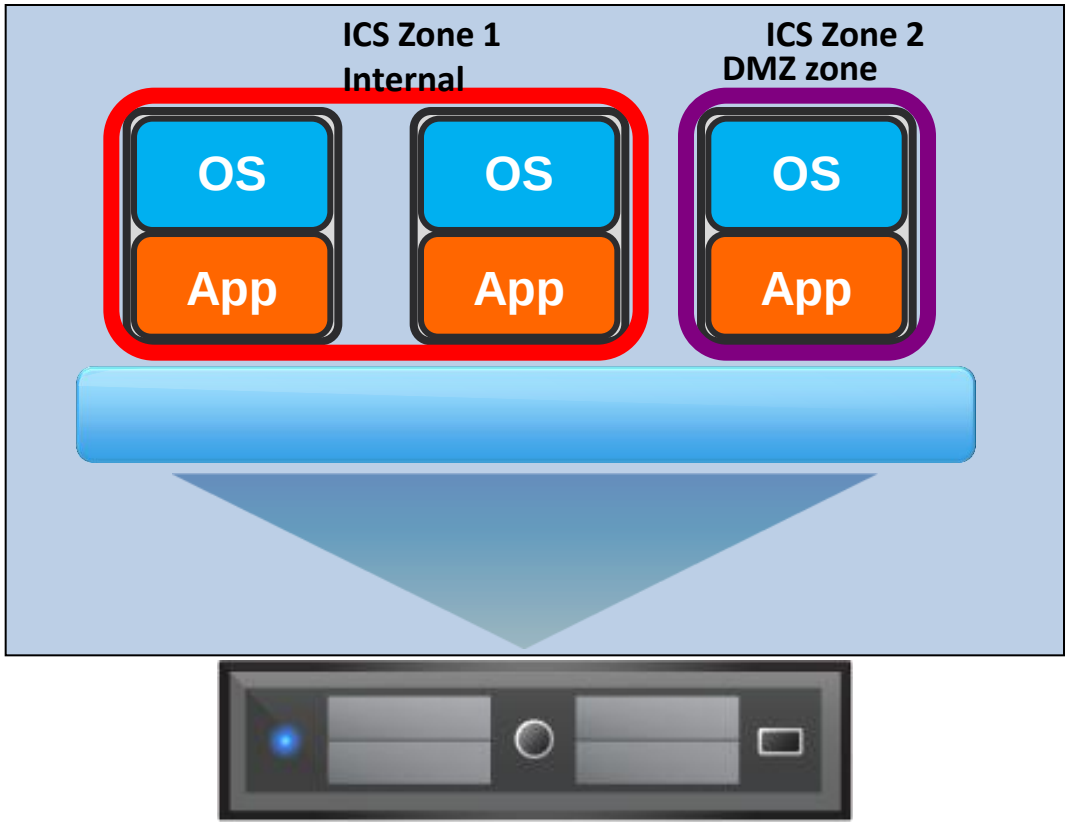


Mixed Mode Single Zone

Zone 1

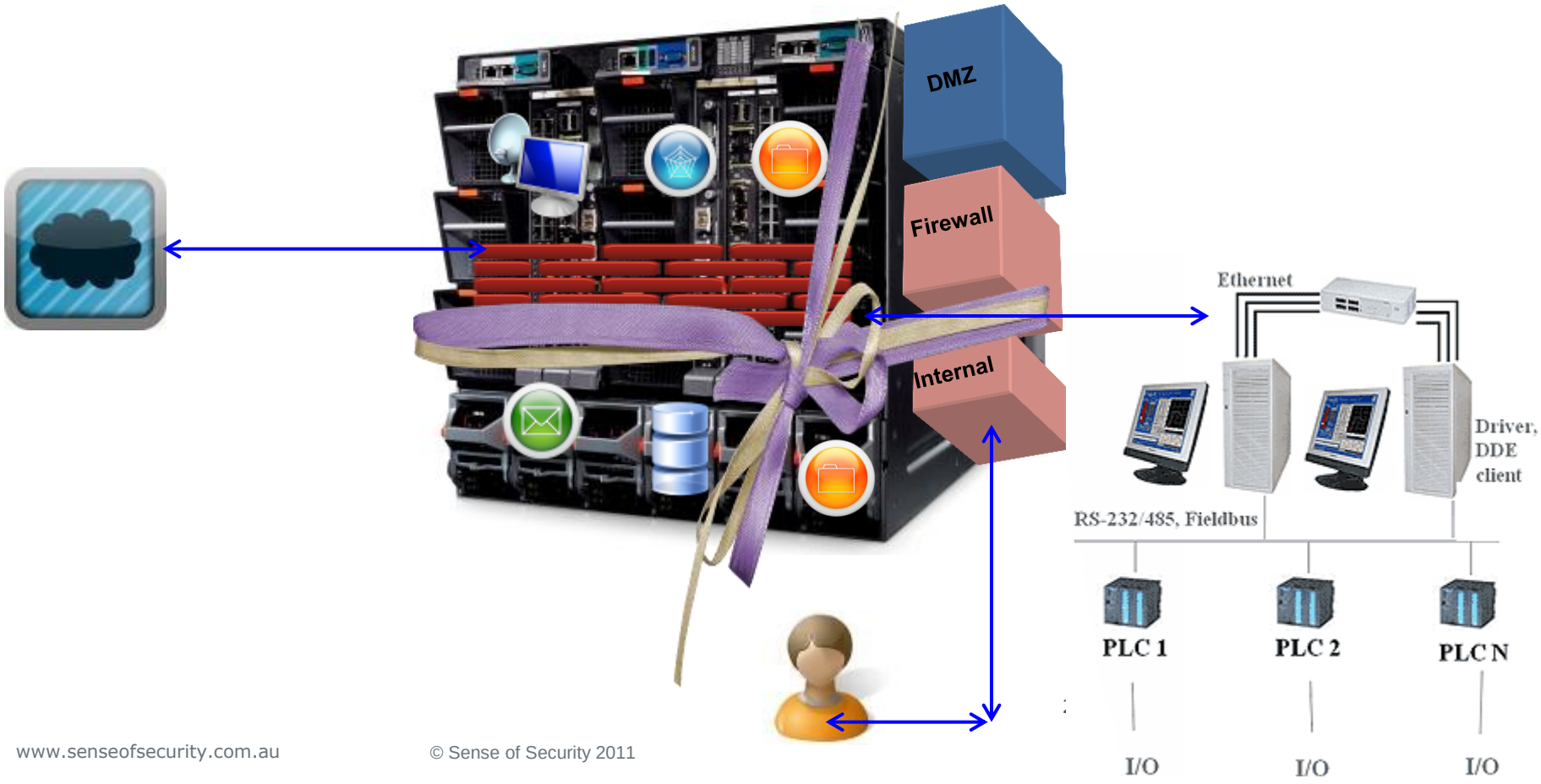


Mixed Mode ICS



How Far Can You Take It?

Company/Facility in a box



Is it getting crowded in there?

NIST Requirements

However, there can be substantial security risks in consolidating multiple services within a single hypervisor. For example, a critical service is usually placed on its own dedicated host so that the host can be secured specifically for that service and so that a compromise of any other service would not impact the critical service. By placing a critical service on a host with other services, both of those goals are impacted. It is particularly risky to place multiple services on a host if they have significantly different security needs. For example, suppose that one service is considered critical and is secured very strongly, while another service on the same host is considered low-impact and is secured relatively weakly. An attacker wanting to compromise the critical service could compromise the low-impact service and use the fact that it is local on the virtual network to attempt to access the critical service or to compromise the hypervisor and thus gain access to the critical service. Organizations that have policies relating to allocation of computer resources should consider virtualization in such policies.

[REF NIST - Guide to Security for Full Virtualization Technologies SP 800-125] [6]

NIST Requirements

Organizations should be aware of how their use of virtualization may affect the security categorization of the physical system. The security categories associated with Federal information system based on three security objectives: confidentiality, integrity and availability. These security categories are described in NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.* The security categorization of a particular information system depends on the potential impact associated with a loss of confidentiality, integrity or availability. If a system hosts guest OSs with different impact levels, the system should be secured in accordance with the highest of those levels. The organization's virtualization security policy should define how combining multiple guest OSs on a single system affects the system's security requirements, both positively and negatively, and which combinations of guest OSs are permitted or prohibited. Organizations may also choose to reduce risk by prohibiting combinations that include resources accessing particular types of information, such as highly sensitive personally identifiable information (PII).[3]

[REF NIST - Guide to Security for Full Virtualization Technologies SP 800-125] [6]

ISM Requirements

Functional separation between servers

Control: 0385; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Where high value servers have connectivity to unsecured public networks, agencies should:

- maintain effective functional separation between servers allowing them to operate independently
- minimise communications between servers at both the network and file system level as appropriate
- limit system users and programs to the minimum access needed to perform their duties.

Control: 0953; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies ensure that functional separation between servers is achieved either:

- physically, using single dedicated machines for each function
- using virtualisation technology to create separate virtual machines for each function in the same security domain.

[REF: Australian Government Information Security Manual - November 2010] [7]

ISM Requirements

Using virtualisation for functional separation between servers

Control: 0841; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Virtualisation technology should not be used for functional separation between servers in different security domains at the same classification.

Control: 0842; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

- Virtualisation technology must not be used for functional separation between servers of different classifications.

[REF: Australian Government Information Security Manual - November 2010] [7]

Stealing a Physical Machine

VERY DIFFICULT

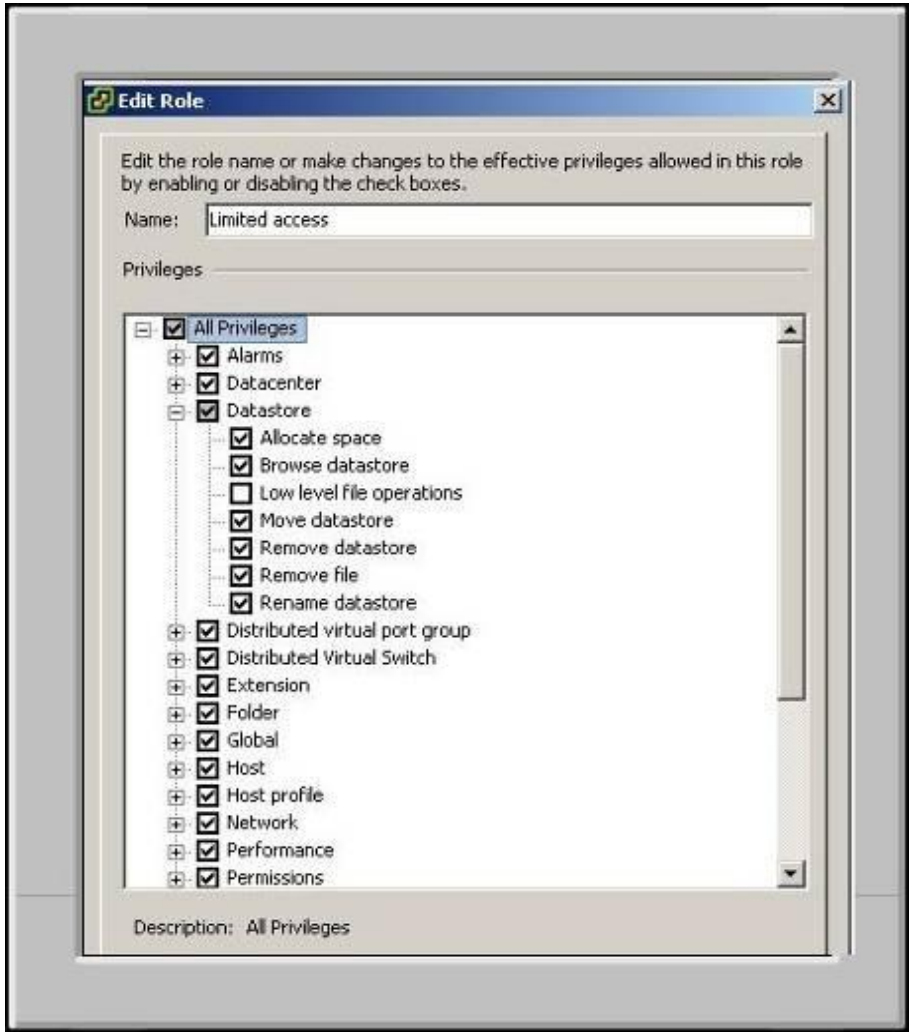
Stealing a Virtual Machine

- Take a snapshot of the machine
- After snapshot virtual disk is unlocked
- Copy to removable media
- Mount VM, access to virtual disk
- If credentials are not known - boot using recovery tool; change admin password
- If credentials are known - power on with player

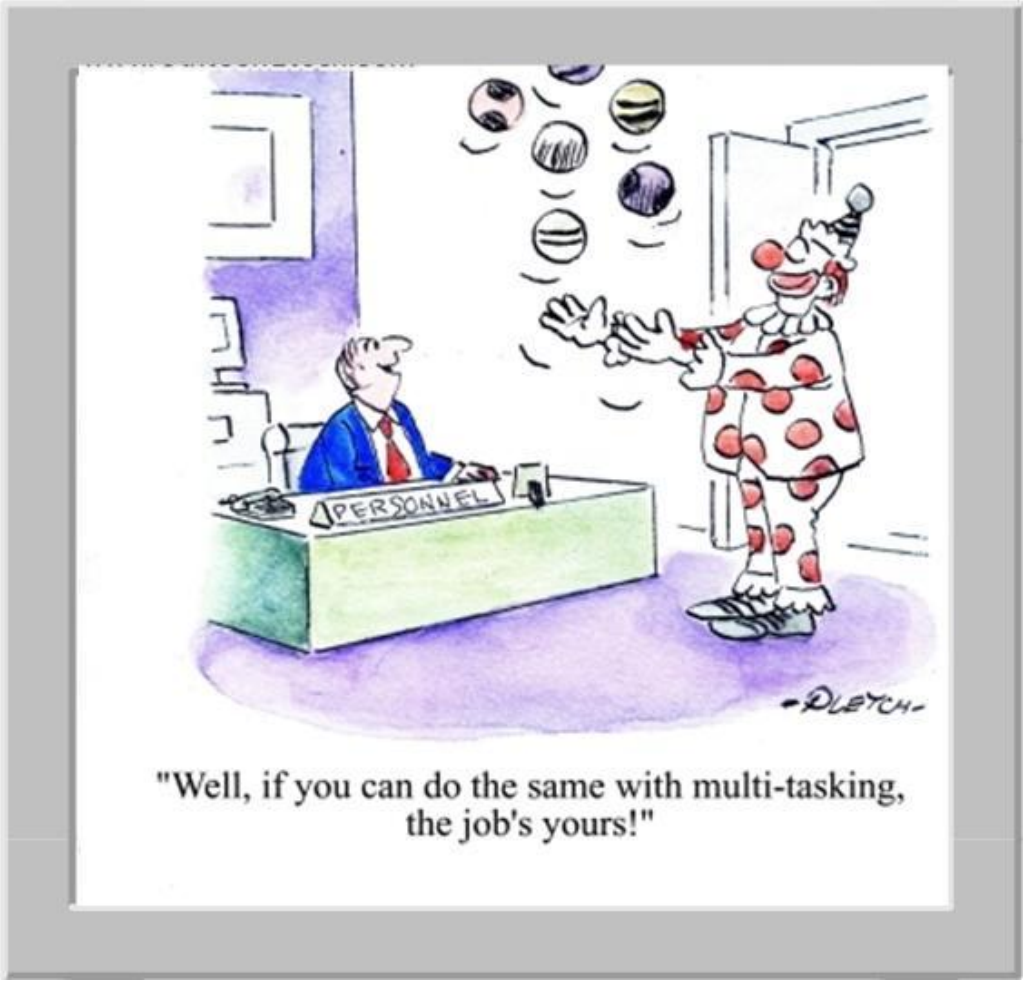
See video at: http://www.senseofsecurity.com.au/consulting/virtualisation-security

Protection

- Encrypt Data
- Improve RBAC – restrict access to low level file ops
- Restrict access to Service Console
- Implement controls for access, accountability, and visibility



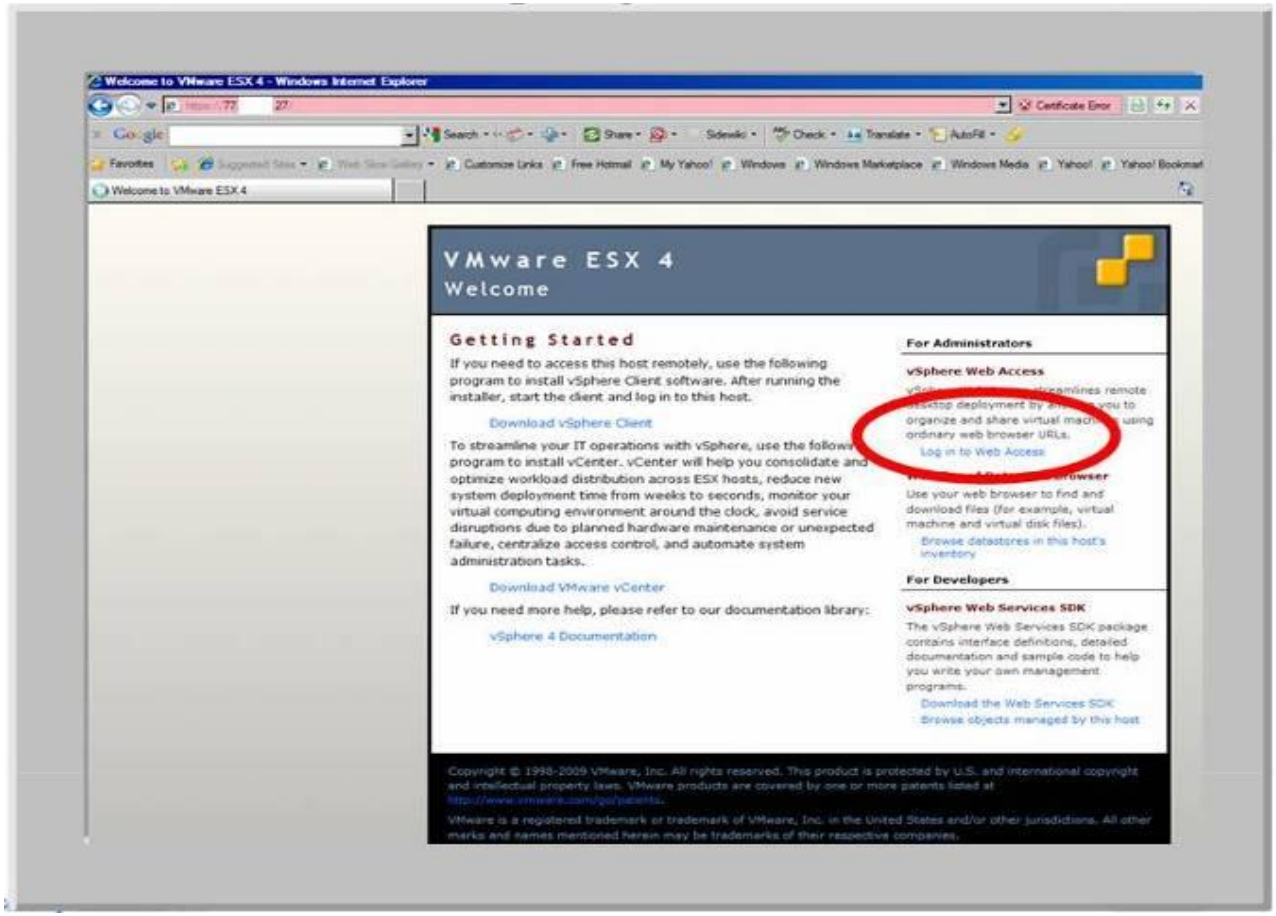
Who manages the system?



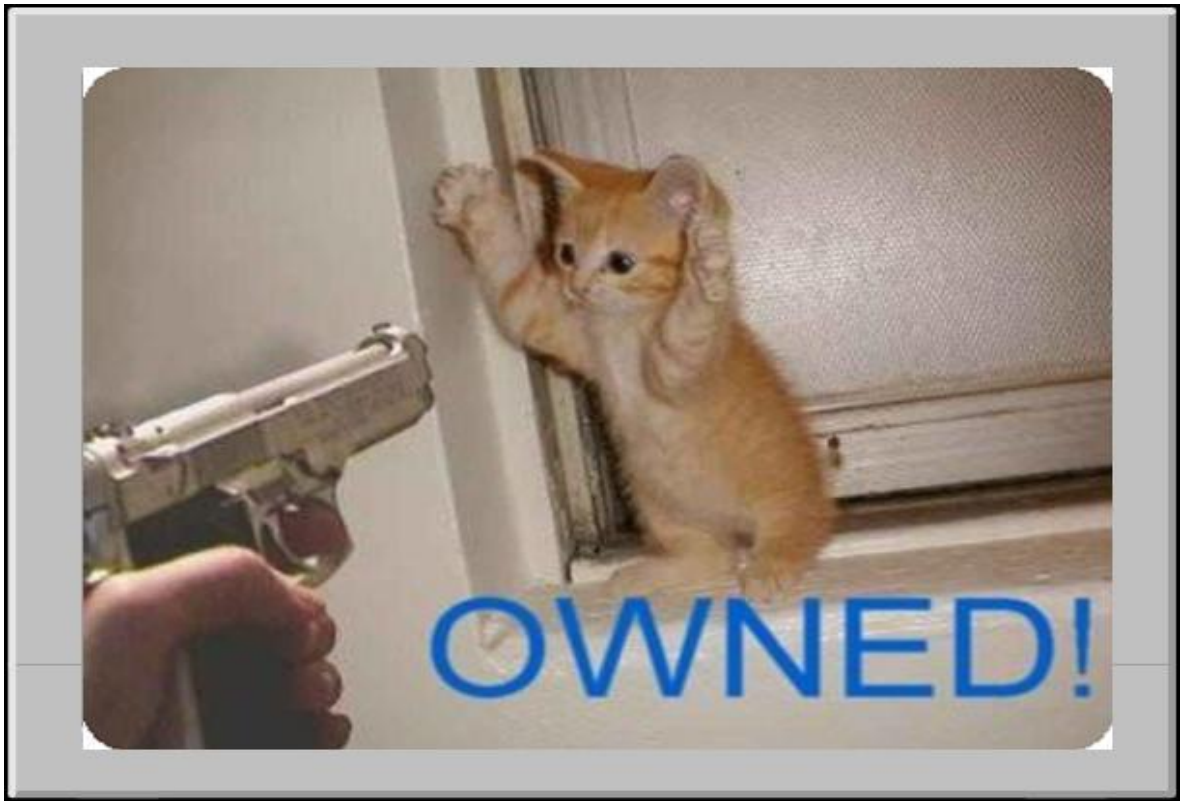
Segregation of Duties

- Server, storage, network, and security duties are collapsed
- Critical considerations:
  - Role-mapping within IT
  - RBAC capabilities of virtualisation platform
  - Layered controls (prevent, detect, respond)
  - Must enforce least privilege
- Roles and Responsibilities
  - Review of discrete responsibilities assigned to roles

Too Accessible?



This is a good start to getting ….



System Components

- Scope – All system components
- For virtualised environments this should include:
  - ANY Virtual Machine
    - Network Component (Vswitch; router)
    - Server (One Primary Function per VM)
    - Application
  - Virtual Appliance
    - Hooks into hypervisor
    - Security Appliances (Firewall, IPS, AV etc)
  - Hypervisor
  - Third Party Components

Hypervisor Protection

- Choice of Hypervisor
  - See industry radar at http://virtualization.info/en/radar/

  - Secure Configuration (Hardening, Disable unnecessary services etc)
  - Encryption of non-console administrative traffic
  - Patch Management, HV is a new dimension
  - Identify new vulnerabilities
  - Restrictive access
  - Effective user authentication
  - Audit trails for all changes

Other Virtualisation Considerations

- Dormant VM's
  - Audit trails required for access to all dormant machines
  - May include sensitive data
  - How do you address retention and destruction?

- Virtual Media
  - SAN/NAS? Management Networks?
  - If NAS will require additional isolation and controls
  - VM's are just files on disks
  - Access controls apply
    - Master images, images with sensitive data
  - Physical controls apply

Other Virtualisation Considerations

- Change Management
  - VMSprawl must be managed particularly for VM's with sensitive data
  - Movement from Dev to Test to Production must be controlled
  - Snapshot and rollback may inadvertently re-instate and non-compliant image
  - Enrolment & retirement must be controlled

Other Virtualisation Considerations

- Audit and Logging
  - The entire environment should be auditable
  - All activity should be logged and monitored
  - Administrators/Auditors should be able to produce compliance reports at any point in time
  - Native and Commercial tools can be used

Audit Items

- Risk Assessment
- Network, LAN, WAN controls
- Infrastructure Readiness & Scope: Dev, UAT, Prod
- System Level & Data Classification
- Documentation: Applicability in policies, standards, procedures
- Specific Controls: Standard specific, deviation management
- Administrative Access; Remote Access
- Logical Access Controls, RBAC
- Intersystem connectivity
- Auditing and Logging
- Backups
- Integrity Monitoring (VM's and VMM)
- Vulnerability Management, Patch Management

[Ref Auditing Security Risks in Virtual IT Systems, ISACA Journal] [8]

Summary of Issues

- Effectiveness of Technical Controls
- Effectiveness of Governance and Risk Management
- Trust & Ownership
- Hypervisors
- Disclosure & Visibility
- Audit, Reporting, Compliance

References

- References:

ANSI/ISA99.02.01-2009 Establishing an Industrial Automation and Control Systems Security Program

Honeywell – Securely integrating multiple systems together as an ICS

Nerc Standard CIP

NIST – Guide to Industrial Control Systems (ICS) Security SP 800-82

Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011 Version 1.
http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

Australian Government Protective Security Policy Framework, AGD, Jan 2011, V1.2
http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Contents

Securing Government Business. Protective Security Guidance for Executives, AGD, June 2010
http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads

References

- References:

Cloud Computing Considerations. DSD, April 2011
http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

IBM XForce 2010 Trends Report, March 2011
http://xforce.iss.net/

Guide to Security for Full Virtualization Technologies SP 800-12, NIST, Jan 2011
http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

Australian Government Information Security Manual - November 2010]
http://www.dsd.gov.au/publications/Information_Security_Manual_2010.pdf

Auditing Security Risks in Virtual IT Systems, ISACA Journal Vol 1, 2011

Thank you

The latest version of this presentation should be downloaded from
http://www.senseofsecurity.com.au/research/presentations

Murray Goldschmidt
Chief Operating Officer
Sense of Security
murrayg@senseofsecurity.com.au
+61 2 9290 4444

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au