Paul Lewis

Practical Steps for E-Infrastructure Security

The Basics : *Definitions of risk*

Definition 1:

The *probability* of an *event* or events occurring that could cause either a positive or negative *impact* upon a system or systems.

Definition 2:

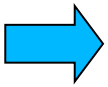
The potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm to the organisation.

Definition 3:

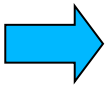
The combination of the probability of an event and its consequence

Information Assets

An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation

Physical Information Asset 

Bank Statements
Utility Bills
Identification document
28m tax records on CDROM

Logical Information Asset 

Database of credit card details
Internal Network configuration data
Employee records

What is a infosec threat?

Threat:

A potential cause to an incident that may result in harm to a system or organisation.

Threat actor - *"A person or group of people who are in a position to attempt to exploit a particular set of Compromise Methods".*

- Foreign Intelligence Services
- Terrorist
- Organised crime
- Investigative journalist
- Hacker / script Kid
- Any others?

Threat type - *"A way of categorising Threat Actors based on their opportunity and Compromise Methods available".*

- Authorised user (normal)
- Authorised user (privileged)
- Service provider
- others?

What is a infosec vulnerability?

Vulnerability:

Weakness of an asset or control that can be exploited by a threat.

Electronic - *"A defect or weakness in the creation, configuration or implementation of a logical asset ".*

- Buffer overflow
- SQL injection

Physical - *"A weakness or defect in a physical structure or system".*

- Unlocked equipment cabinet doors
- Unprotected communication cables

Human - *"A weakness in a persons knowledge, education or training".*

- Easy to guess passwords
- Password sharing

Procedural - *"The omission or subversion of a security process"*

- Verification of security checks
- Missed software patches

What's important to you?

How Do I Manage Infosec Risk?

- Checklists
  - Security Technical Implementation Guides (STIGS) and NSA Guides
  - HMG Infosec standards
  - SANS – Security consensus operational readiness evaluation (SCORE)
- Processes
  - COSO
  - CRAMM v5.2 (links directly into ISO27001)
  - ISF method
  - OCTAVE
- Standards
  - P800-30 (NIST)
  - ISO/IEC 13335-2 (now called ISO/IEC 27005)
  - Payment Card Industry Data Security Standards (PCI DSS)
- **Don't** Manage Them!

Council on Cybersecurity

Top 20 critical security controls:

Critical control 1 - Inventory of authorised and unauthorised devices
Critical control 2 - Inventory of authorised and unauthorised software
Critical control 3 - Secure configurations for hardware and software
Critical control 4 - Continuous vulnerability assessment and remediation
Critical control 5 - Malware defences
Critical control 6 - Application software security
Critical control 7 - Wireless device control
Critical control 8 - Data recovery capability
Critical control 9 - Security skills assessment and appropriate training to fill gaps
Critical control 10 - Secure configurations for network devices

Risk Reporting

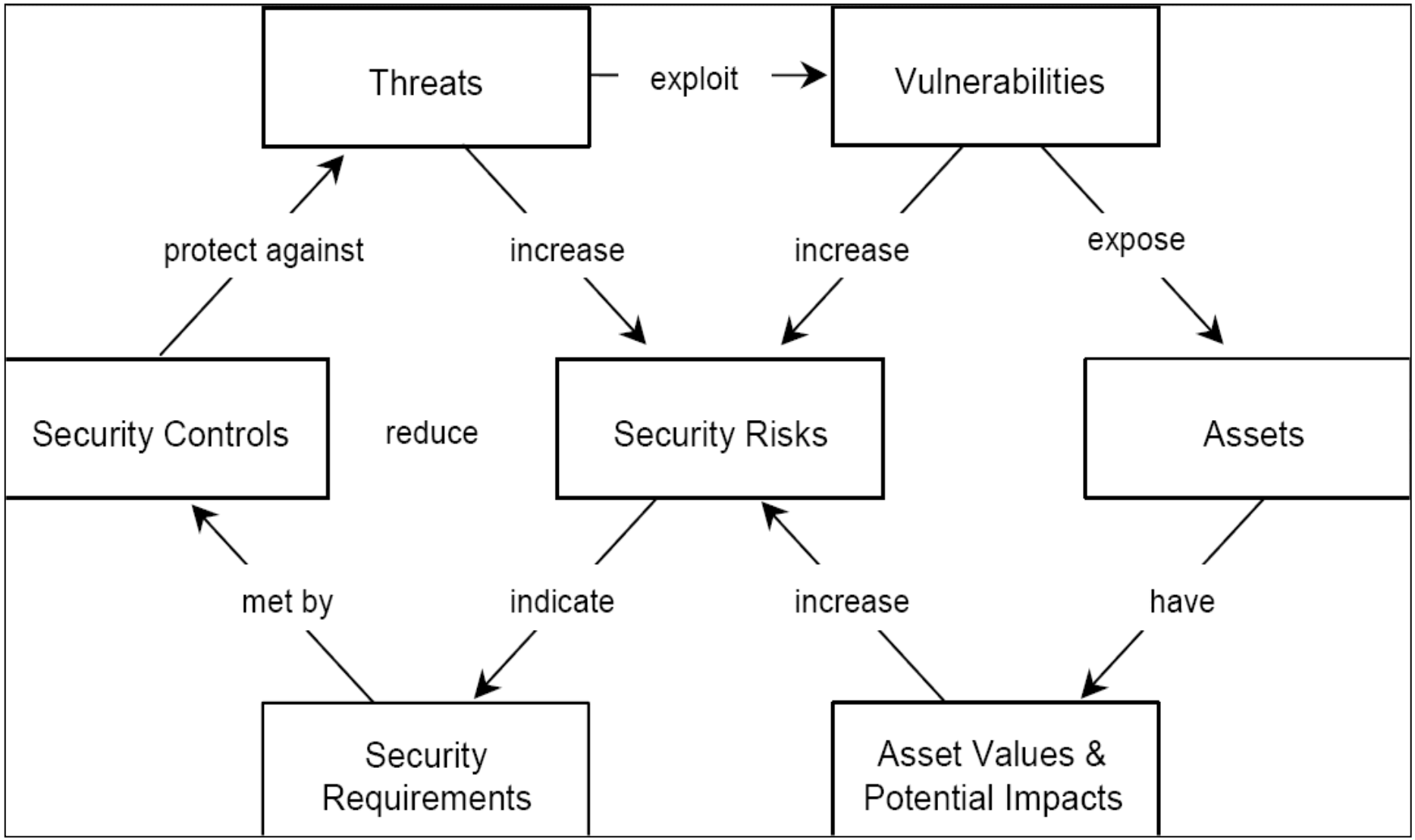
Generally Information risks are communicated via written reports via lists of problems, impacts, mitigations and cost.

Table 2: Results of the evaluation of infectious waste handling practices using the PRA technique. Example: Segregation operation.

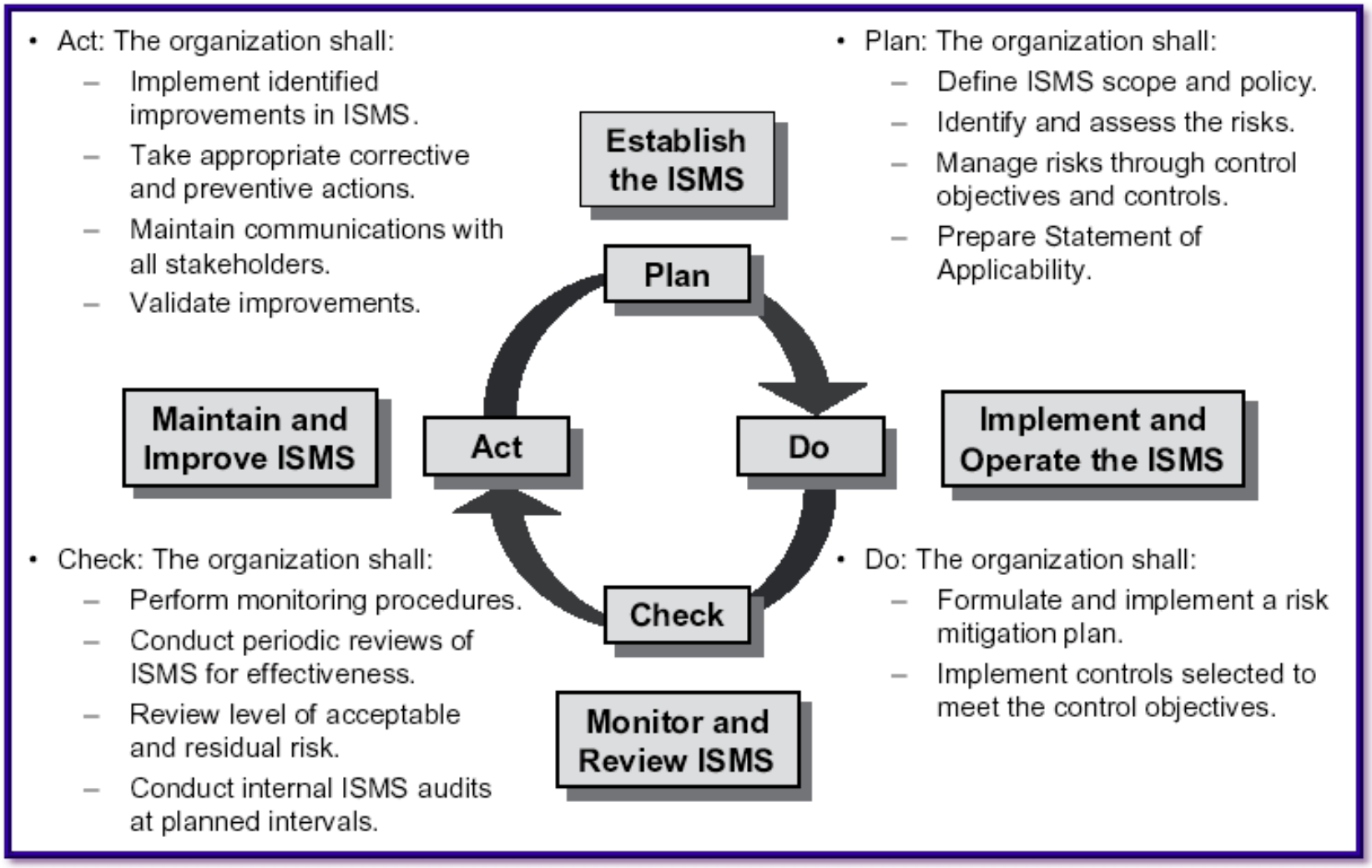
System or subsystem: Health-care Establishment						
Handling practice: Segregation Operation						
Objective: Separation and Identification of the Waste.						
Date:						
Procedure	**Failure**	**Detection method**	**Consequence**	**Severity of consequence**	**Probability of occurrence**	**Corrective actions**
All wastes have to be contained in plastic bags or containers appropriately identified as close as possible to where they were generated.	* Containers distant from the source of generation of waste.	* Inspection at the source of generation of waste.	* Discourage a proper segregation of waste.	I	L	* To identify all the sources of generation of infectious waste and to locate as close as possible to them properly identified bags or containers.
	* Containers and plastic bags inadequately identified.	* Inspection at the source of generation of waste.	* Increase of the amount de infectious waste.	II	L	

Is this always the correct way to communicate risk?

AS/NZ 4360:2004 *Risk Management* *(Superseded by 31000:2009)*



Plan, Do, Check, Act Loop



12.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

12.6.1 Control of technical vulnerabilities

Control

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Implementation guidance

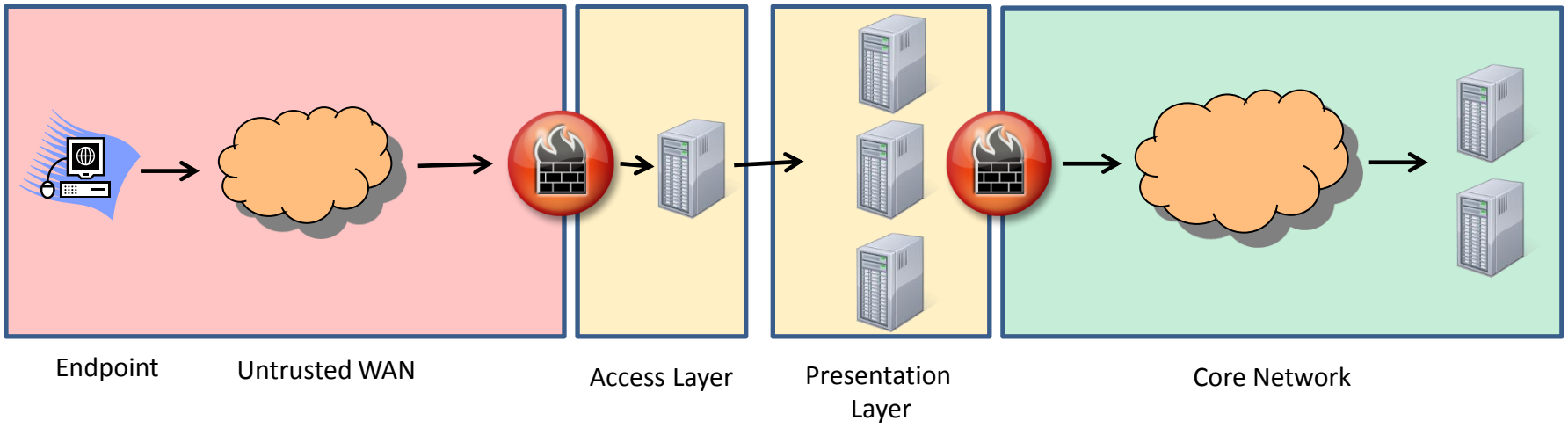
A current and complete inventory of assets (see 7.1) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organization responsible for the software.

Appropriate, timely action should be taken in response to the identification of potential technical

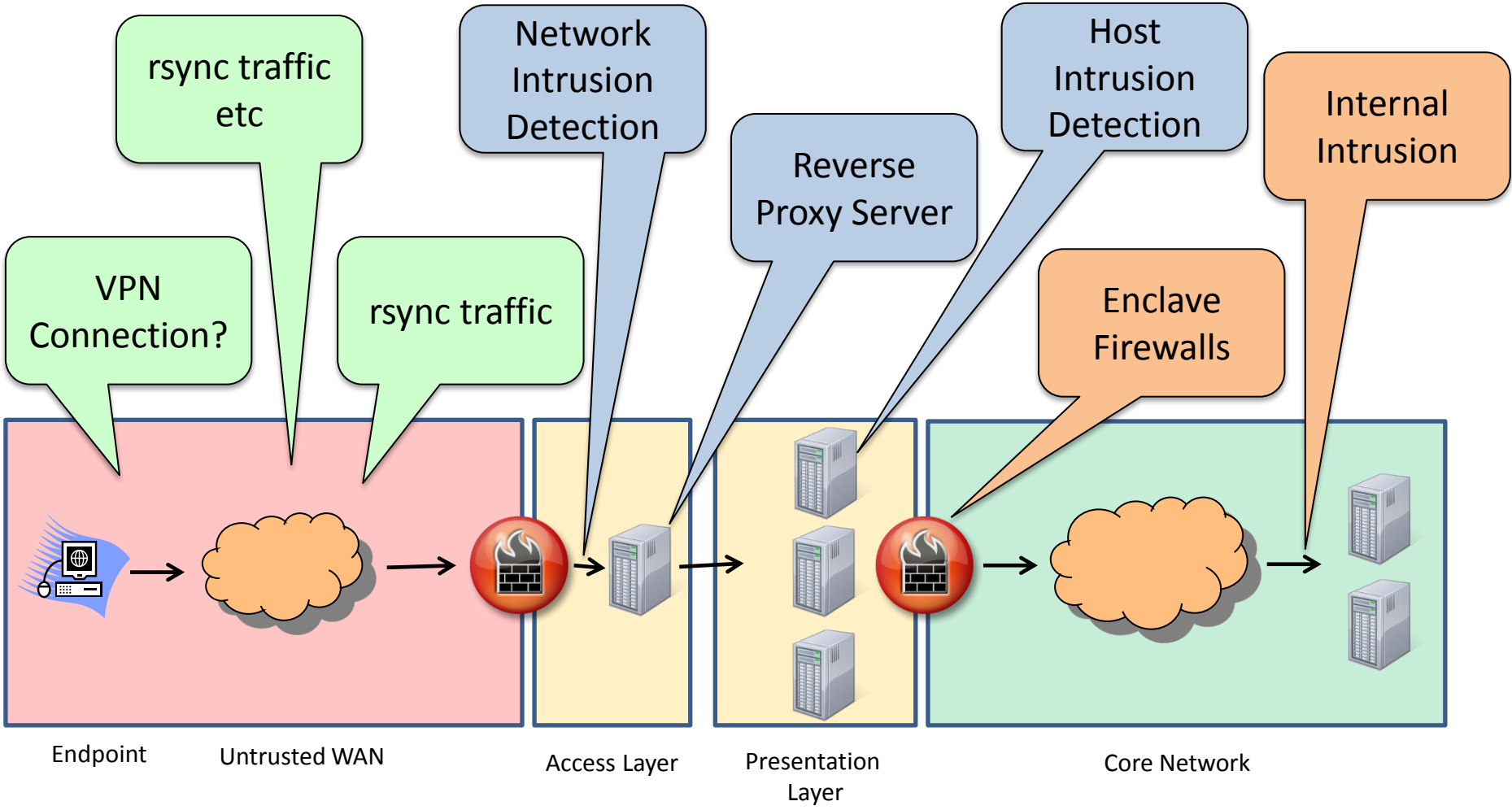
Perimeter Control

The external architecture is split across 2 distinct layers. Access layer the provides access to authorised users and presentation layer that provides a limited view of the core systems

In addition to the external perimeter controls, separation or security zoning can also be adopted within layers, known as ‘enclaves’

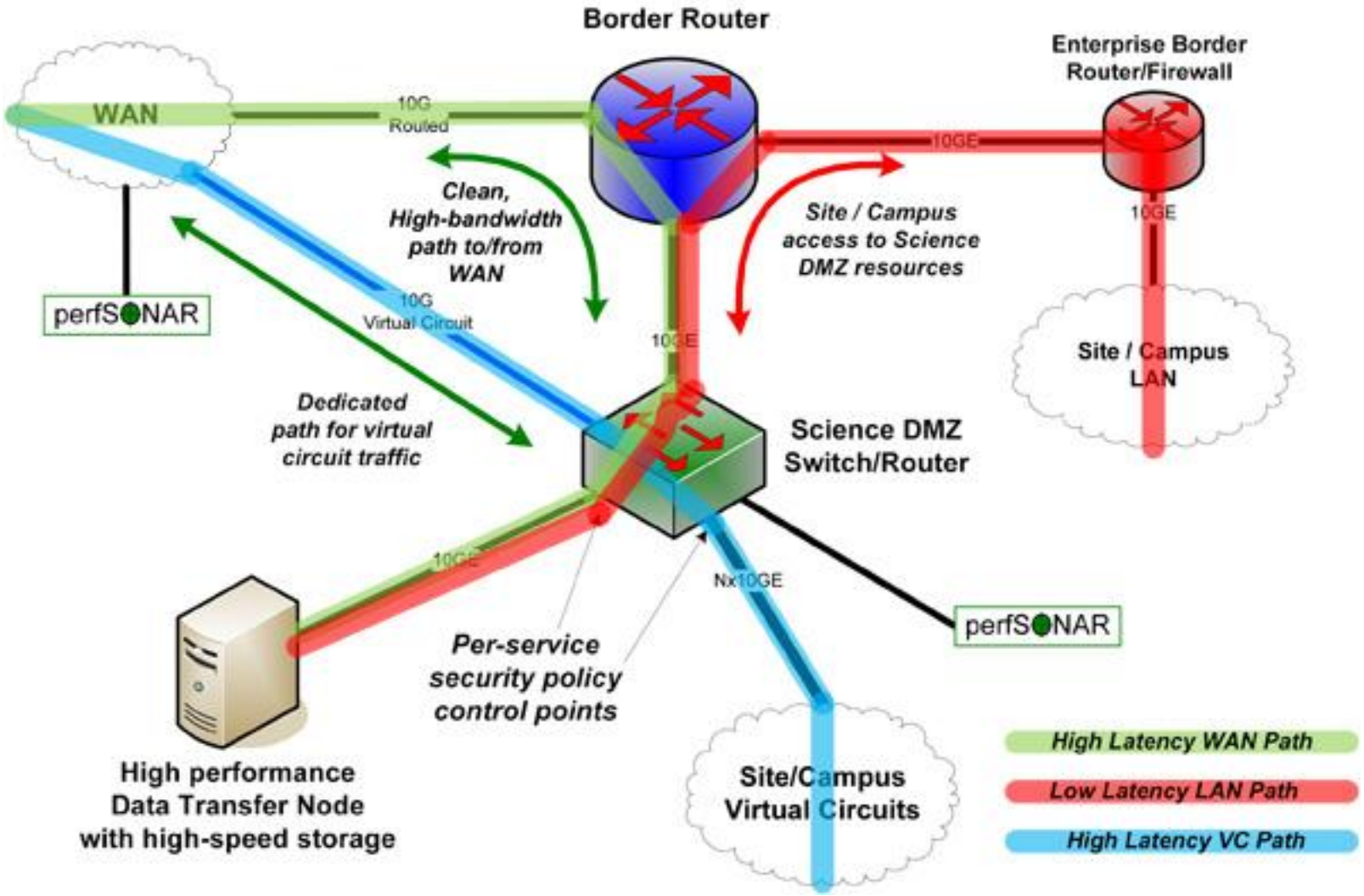


Perimeter Control



Science DMZ?

(http://fasterdata.es.net/science-dmz/)



Virtual Private Networks

VPN's provide a range of services that are required by the information assurance CIA principles.

Confidentiality - If the traffic is sniffed or intercepted all that is obtained is encrypted packets.

End point Integrity – The users of the VPN can authenticate each other identity and ensure the endpoint integrity.

Message integrity – Any tampering with transmitted messages can be detected.

VPN's can run in transport mode (only the payload is encrypted) or tunnel mode. (the whole datagram is encrypted).

IPSEC – IP Security generally the most used way to establish a VPN
SSL/TLS – Secure Sockets Layer/Transport Layer Security - normally used in web browsers
PPTP – Point to Point Tunneling Protocol - Microsoft implementation of VPN

In August 2013 the Syrian Electronic Army (SEA) undertook a number of operations to deface or disrupt a number of high profile websites around the world.

The difference is SEA didn’t attack the victims directly….

Attack No.1 – Outbrain Content Recommendation provider

- On the evening of August 14th, a phishing email was sent to all employees at Outbrain purporting to be from Outbrain's CEO.
- The email contained a link from a prominent news source, which redirected to a page asking Outbrain employees to input their credentials.
- SEA **Redirected** referrals for washtonpost.com , cnn.com and time magazine to SEA websites.

https://admin1.outbrain.com:8443/flightmanager/groupSettings.action#groupId=8633&widgetId=147

DomainTools.com Whois

GROUP SETTINGS TOOL

timemag (8633)

Find by URL: http://time.com/word/

Find by ID:

Search

DRAFT-PROD INTERFACE

Copy to Draft | View Draft

Check Cache

Group Info

ID: 8633

Name: timemag

Widget ID: SB_3

Widget Description: Sidebar 3

Xpath Tool

Show only effective settings | Basic settings | Xpath Tool | Categories | Organic Recs Optimizer | Search

ID	Name	Value	Origin
	Category: Widget settings		
16	Recommend paid links?	false	DEFAULT
21	Total number of recs	3	WIDGET
38	Open recommendation in a new tab	true	DEFAULT
59	Paid links on top?	true	DEFAULT
81	Max paid recs	0	WIDGET
88	Widget structure	box	WIDGET
107	Max organics recs		DEFAULT
109	Request type	doc_recs	DEFAULT
128	Enable paid label?	false	DEFAULT
131	Title character limit	1000	DEFAULT
141	Paid links positions		DEFAULT
174	Widget whitelist ID		DEFAULT
175	Max paid recs from advertiser		DEFAULT
176	**First header**	**<script type="text/javascript"> var ...**	**GROUP**
177	Second header		DEFAULT
187	Paid label copy	Paid Distribution	DEFAULT
229	Publisher custom widget name		DEFAULT
263	Widget statistics	false	DEFAULT
356	Paid section first	false	DEFAULT

Setting Info

nanoOrganicsHeader

Description

First header in a widget.

admin1.outbrain.com 10.20.65.82


md5.rednoize.com - r.:.
Twitter & Facebook A...
://edition.cnn.com)
Cache Health
Xpath Tool
Categories
mendationLocationString
iption
nge the string for the location of
urce of recommendation (use
URCE_NAME for the source .
he string (source) after each
mmendation , for example
($SOURCE_NAME) will put the source's
@id='cnnContentContainer']/h1","...
TEMPLATE

Ad Nauseam

1. Check what you have;
2. Check what is important;
3. Check what are your risks are;
4. Choose your protection methods;
5. (Use free stuff first!)
6. Implement the protections;
7. Check they work;
8. Come back in 6 months and do 1 -7 again!

Questions?