Security Architecture & Risk Assessment

April 28, 2005

André Carrington, P.Eng, CISSP, CISM

BEDROCK security services

What is critical to improve security in your organization?

- Top management support
- Alignment with business objectives
- Business case “value” analysis
- Involvement of staff & business process owners
- Sufficient resources
- Being prepared for incidents
- Managing expectations

Agenda

- Threats and risks
- Threat-Risk & Gap assessment
- Enterprise security architecture
- Wireless security architecture

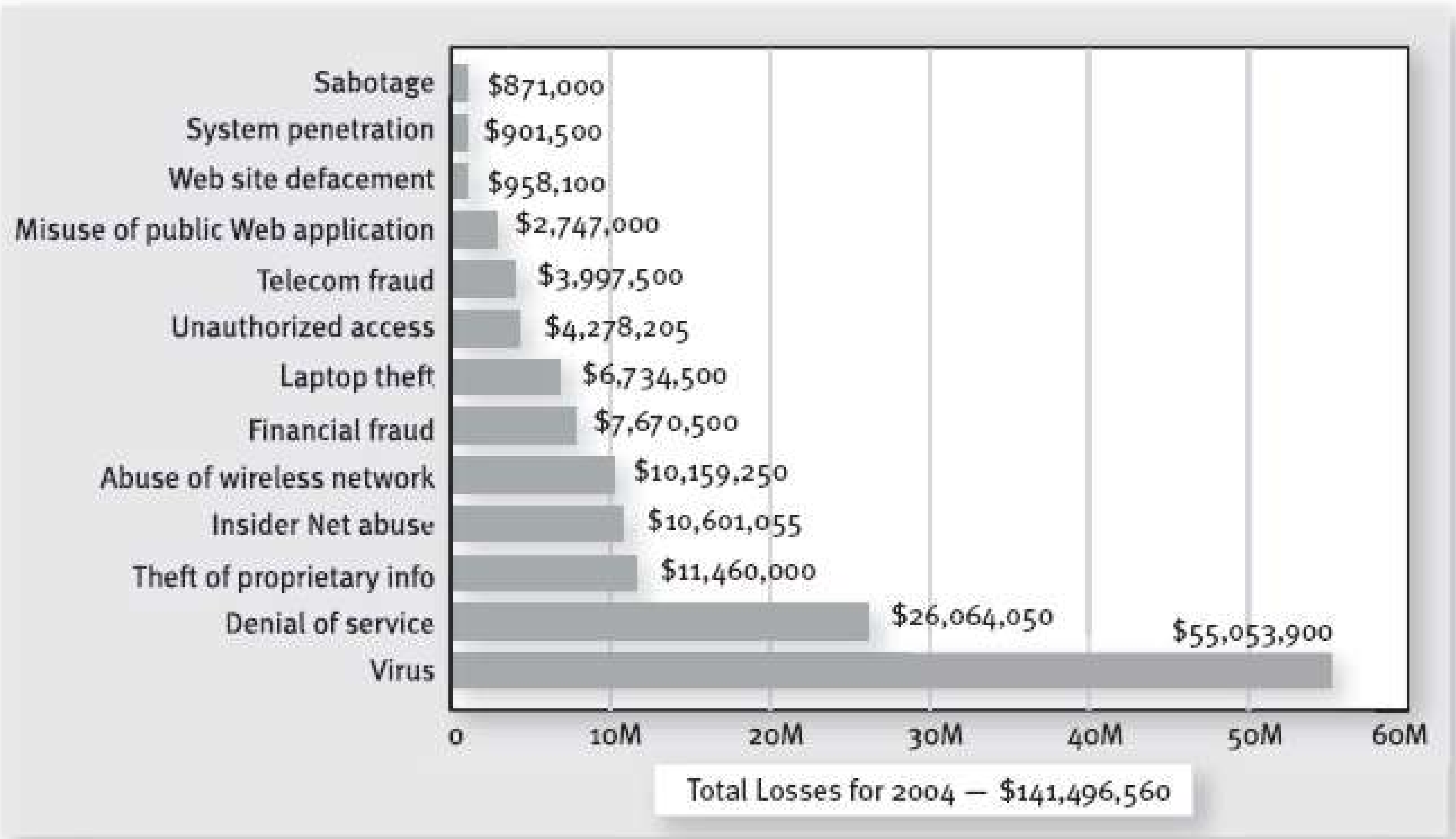
Recent Incidents

- Bank of America loses tapes re 1.2 million federal workers
  - Ameritrade loses backup tapes in shipping re 200,000 clients
- Keyloggers & wire transfer fraud in attempted theft of £220m from Sumitomo Mitsui bank
- Bank of America sued by a customer whose Trojan-infected computer permitted an unauthorized transaction for USD $90,000
  - Phishing and Trojans cause losses of £12m for UK banks in 2004
- Theft of 1.4 million credit cards from DSW Shoe data warehouse
  - Sovereign bank is suing DSW Shoe with respect to the VISA CISP

Recent Incidents II

- DNS attacks redirect/capture traffic to financial & retail web sites
  - americanexpress.com; citicards.com; adp.com; walmart.com; cnn.com; etc.
- Lowe's credit-card system attacked through wireless access points
- ChoicePoint, a background check company, provided information on 145,000 consumers to fraudulent businesses; ~750 confirmed ID thefts.
- Former IT Manager indicted on computer crime charges
  - Records of many similar cases are found on the US DOJ web site

Losses reported



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Limitations of data

- Aggregate data
  - Not specific to industry, region
- Coarse data
  - Few specifics on controls that failed and the IT infrastructure & services
- Reputation loss/impact difficult to quantify
- Impact variables
  - media spin; law suits; expectations/brand
- Operational losses not accurate

Agenda

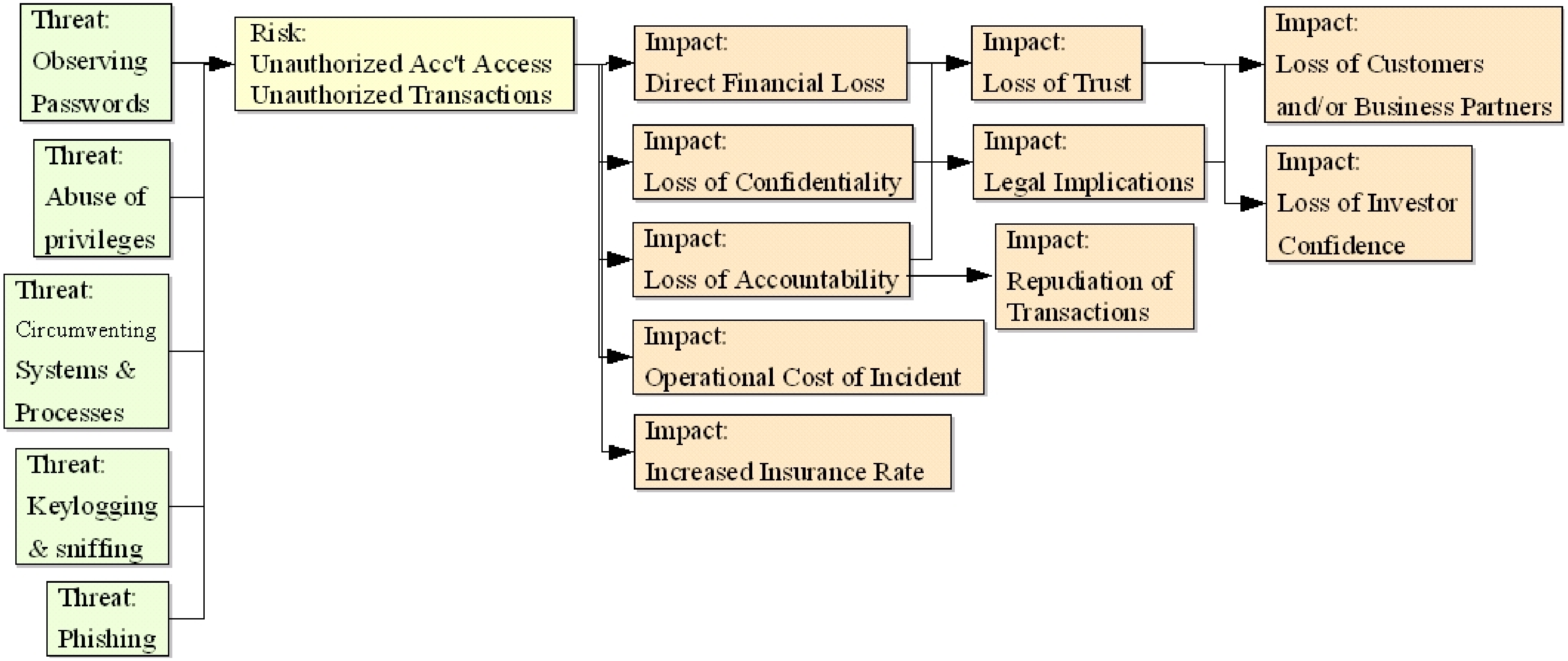
Threats and risks

Threat-Risk & Gap assessment

Enterprise security architecture

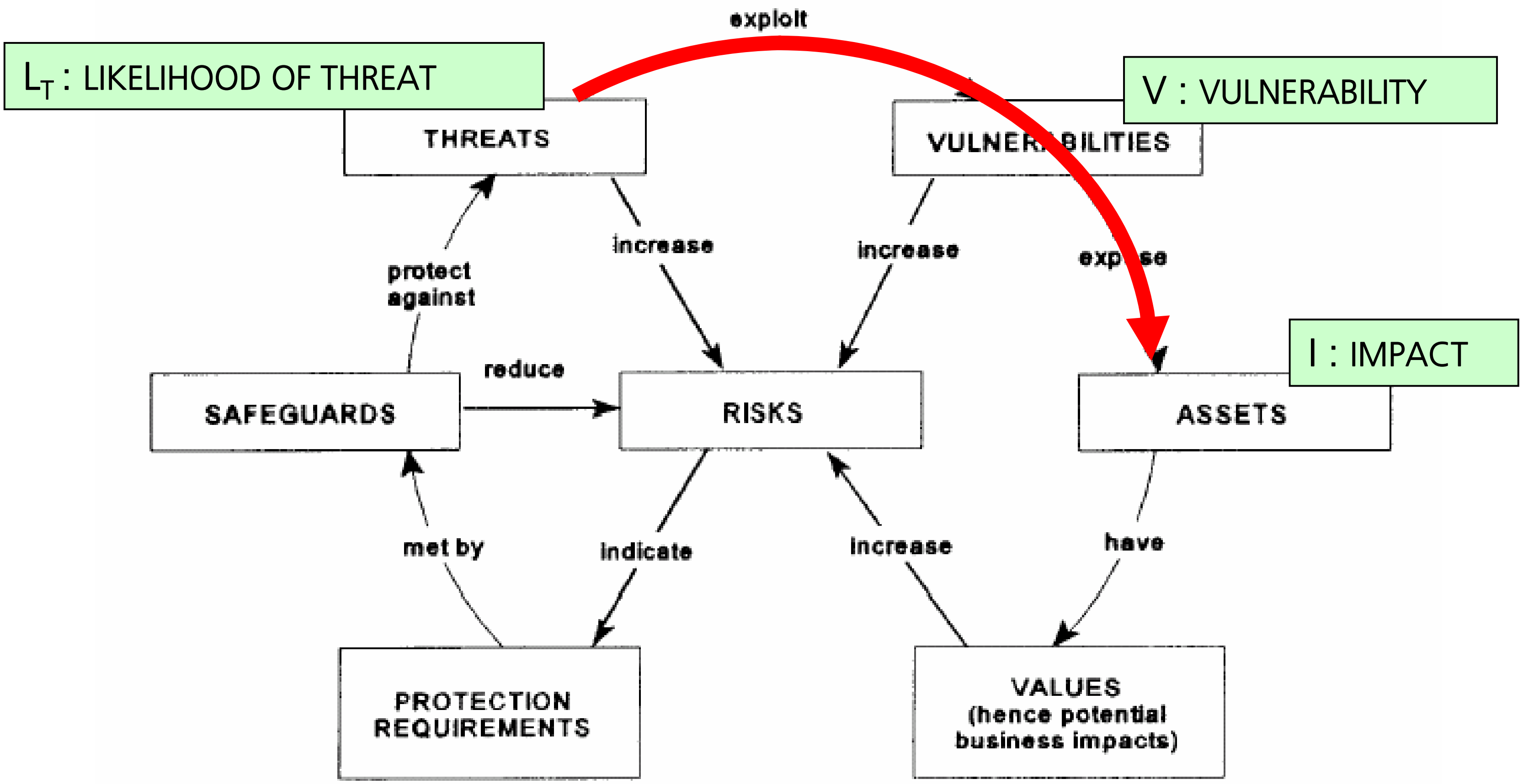
Wireless security architecture

Threat-Risk Models


Threat: Observing Passwords
Threat: Abuse of privileges
Threat: Circumventing Systems & Processes
Threat: Keylogging & sniffing
Threat: Phishing
Risk: Unauthorized Acc't Access Unauthorized Transactions
Impact: Direct Financial Loss
Impact: Loss of Confidentiality
Impact: Loss of Accountability
Impact: Operational Cost of Incident
Impact: Increased Insurance Rate
Impact: Loss of Trust
Impact: Legal Implications
Impact: Repudiation of Transactions
Impact: Loss of Customers and/or Business Partners
Impact: Loss of Investor Confidence

Source: Threat-risk model concept developed by André Carrington.

Threat-Risk Model



Source: ISO 13335 (GMITS)

Likelihood vs. Impact

		I : IMPACT		
		Low	Medium	High
L_T : LIKELIHOOD OF THREAT	High	5	8	9
	Medium	3	6	7
	Low	1	2	4

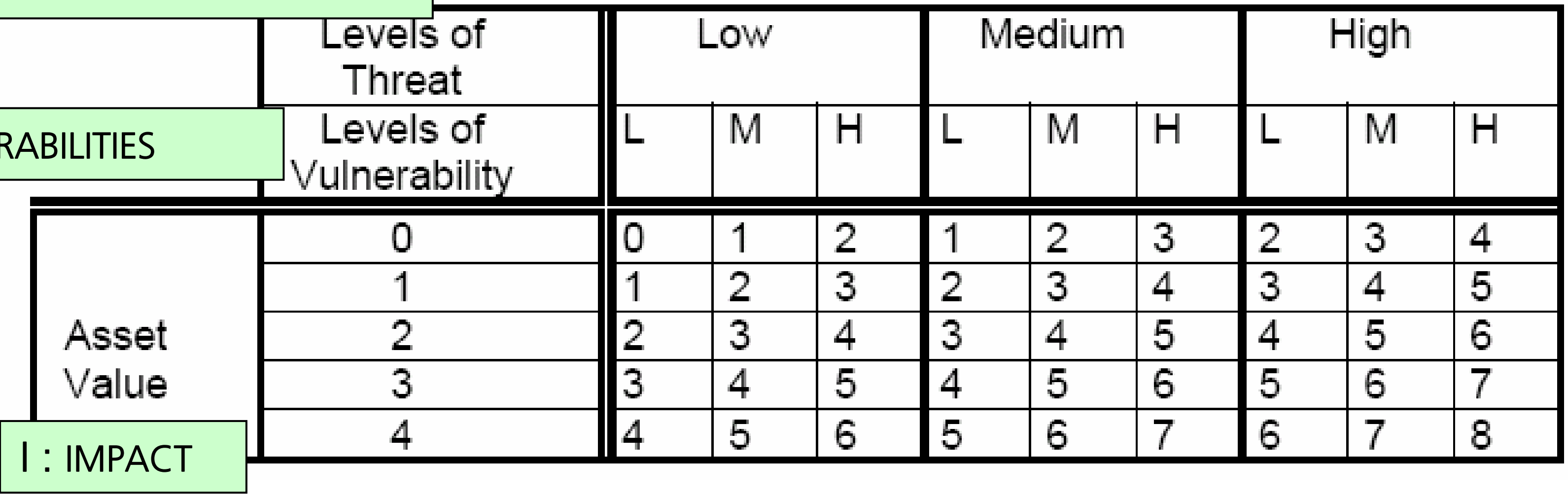
Source: RCMP TRA Guide

More complex tables

L_T : LIKELIHOOD OF THREAT

V : VULNERABILITIES

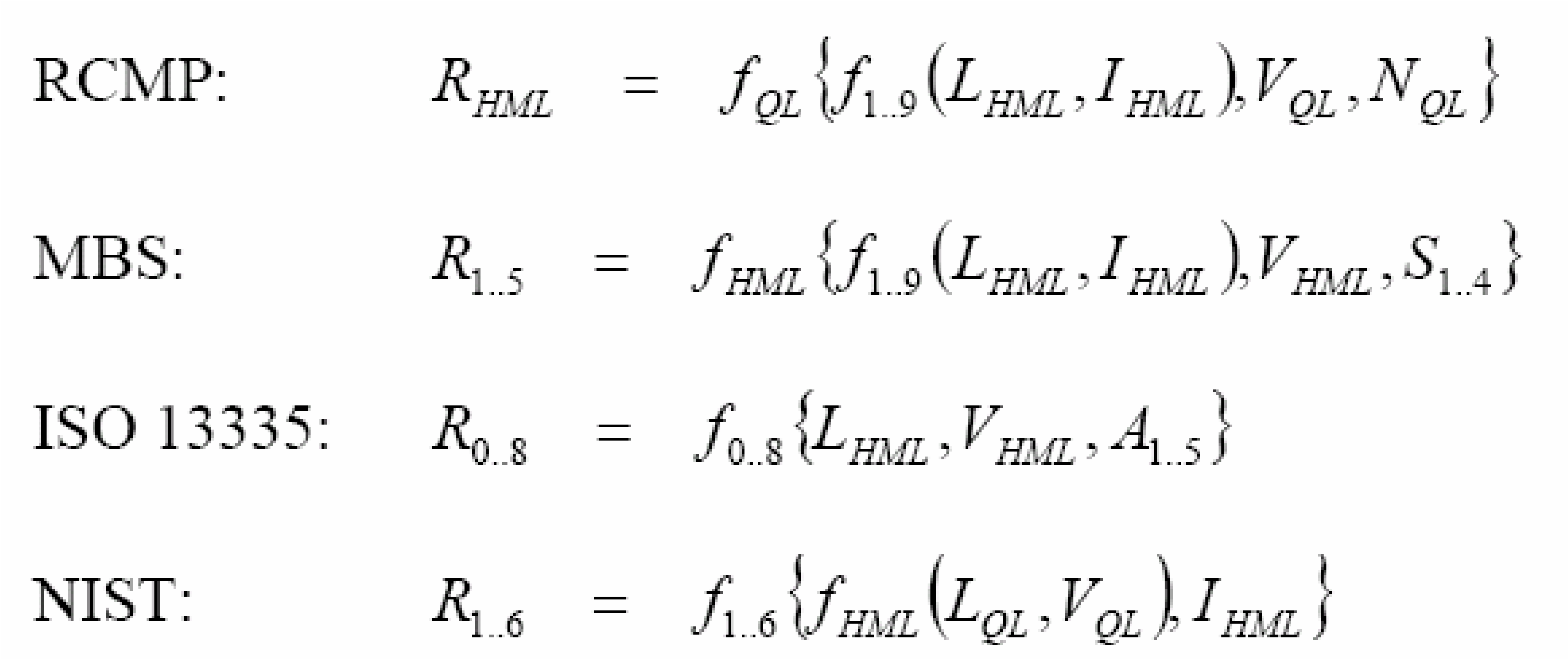
I : IMPACT



	Levels of Threat	Low			Medium			High		
	Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Source: ISO 13335 (GMITS)

Formulae



RCMP: $R_{HML} = f_{QL}\left\{f_{1..9}\left(L_{HML}, I_{HML}\right), V_{QL}, N_{QL}\right\}$

MBS: $R_{1..5} = f_{HML}\left\{f_{1..9}\left(L_{HML}, I_{HML}\right), V_{HML}, S_{1..4}\right\}$

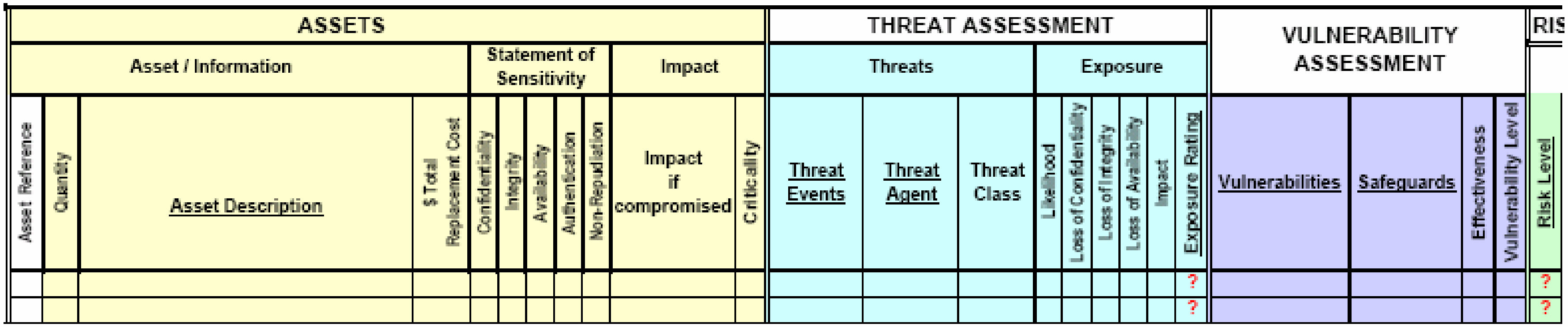
ISO 13335: $R_{0..8} = f_{0..8}\left\{L_{HML}, V_{HML}, A_{1..5}\right\}$

NIST: $R_{1..6} = f_{1..6}\left\{f_{HML}\left(L_{QL}, V_{QL}\right), I_{HML}\right\}$

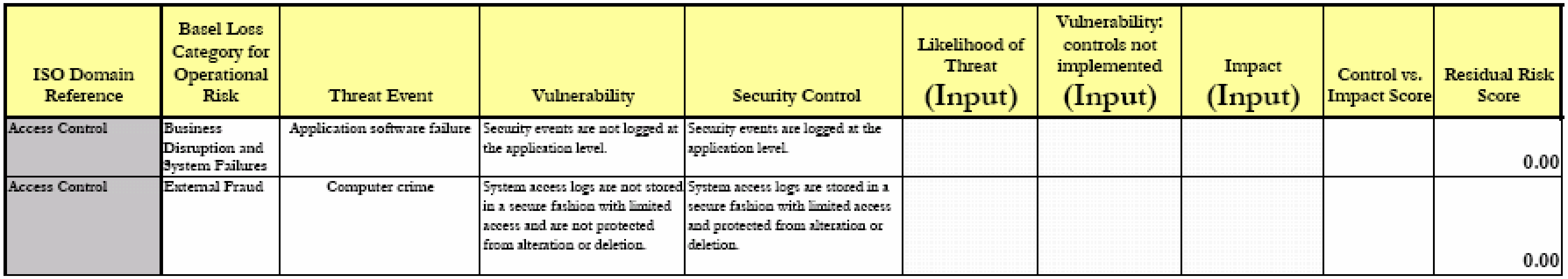
Variables: L=Likelihood; I=Impact; V=Vulnerability; N=Nature of threat; S=Safeguards; A=Asset value
Values: QL=Qualitative; HML=high, medium, low; 1..n=rank from 1 to n

Source: Formulae developed
by André Carrington.

Tools to automate & guide



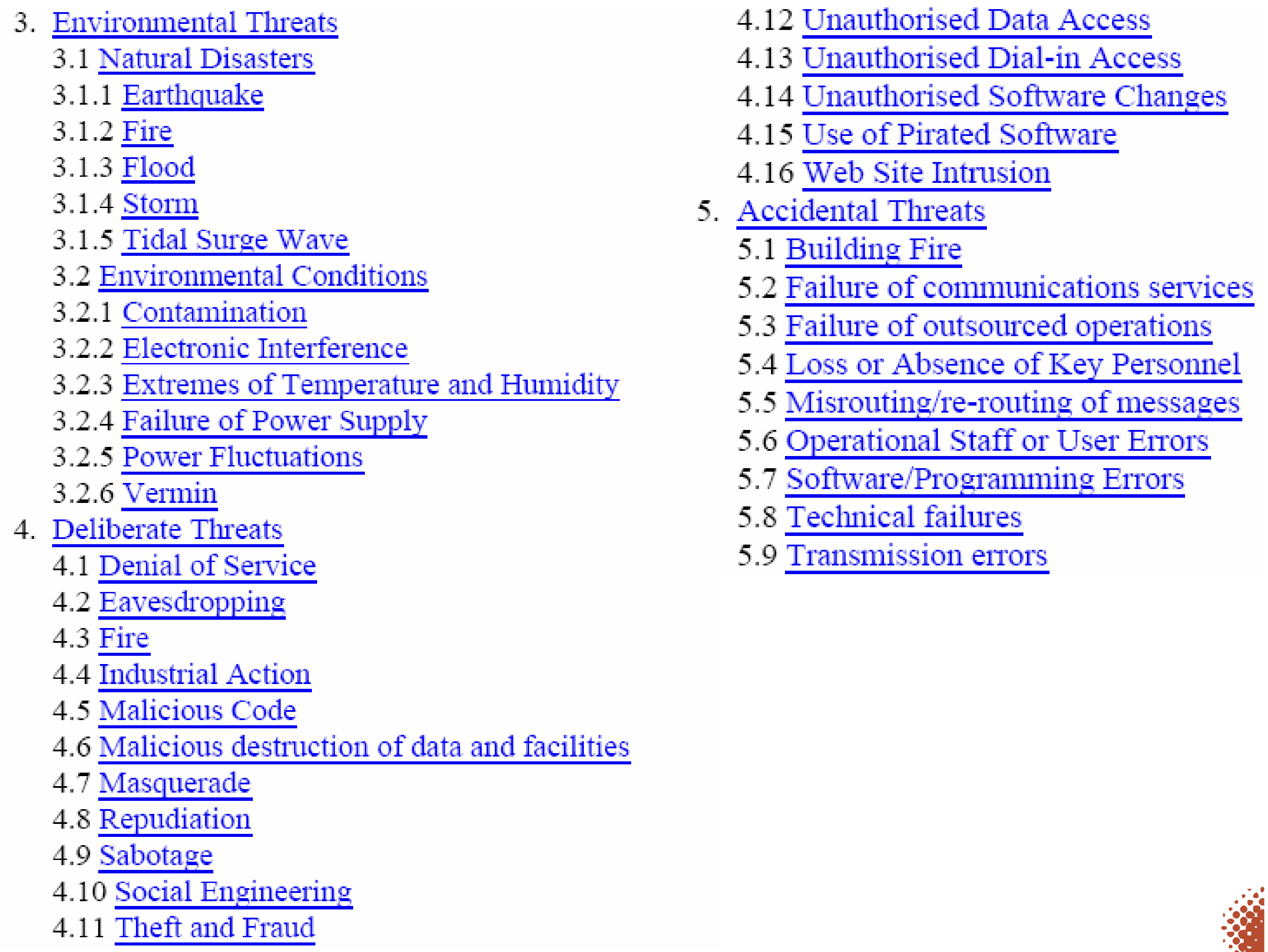
ASSETS											THREAT ASSESSMENT									VULNERABILITY ASSESSMENT				RIS
Asset / Information				Statement of Sensitivity					Impact		Threats			Exposure										
Asset Reference	Quantity	Asset Description	$ Total Replacement Cost	Confidentiality	Integrity	Availability	Authentication	Non-Repudiation	Impact if compromised	Criticality	Threat Events	Threat Agent	Threat Class	Likelihood	Loss of Confidentiality	Loss of Integrity	Loss of Availability	Impact	Exposure Rating	Vulnerabilities	Safeguards	Effectiveness	Vulnerability Level	Risk Level
																			?					?
																			?					?



ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Likelihood of Threat (Input)	Vulnerability: controls not implemented (Input)	Impact (Input)	Control vs. Impact Score	Residual Risk Score
Access Control	Business Disruption and System Failures	Application software failure	Security events are not logged at the application level.	Security events are logged at the application level.					0.00
Access Control	External Fraud	Computer crime	System access logs are not stored in a secure fashion with limited access and are not protected from alteration or deletion.	System access logs are stored in a secure fashion with limited access and protected from alteration or deletion.					0.00

Source: Ontario MBS TRA tool
BITS Basel Kalculator [sic]

Tools also provide lists



3. Environmental Threats
   - 3.1 Natural Disasters
   - 3.1.1 Earthquake
   - 3.1.2 Fire
   - 3.1.3 Flood
   - 3.1.4 Storm
   - 3.1.5 Tidal Surge Wave
   - 3.2 Environmental Conditions
   - 3.2.1 Contamination
   - 3.2.2 Electronic Interference
   - 3.2.3 Extremes of Temperature and Humidity
   - 3.2.4 Failure of Power Supply
   - 3.2.5 Power Fluctuations
   - 3.2.6 Vermin
4. Deliberate Threats
   - 4.1 Denial of Service
   - 4.2 Eavesdropping
   - 4.3 Fire
   - 4.4 Industrial Action
   - 4.5 Malicious Code
   - 4.6 Malicious destruction of data and facilities
   - 4.7 Masquerade
   - 4.8 Repudiation
   - 4.9 Sabotage
   - 4.10 Social Engineering
   - 4.11 Theft and Fraud
   - 4.12 Unauthorised Data Access
   - 4.13 Unauthorised Dial-in Access
   - 4.14 Unauthorised Software Changes
   - 4.15 Use of Pirated Software
   - 4.16 Web Site Intrusion
5. Accidental Threats
   - 5.1 Building Fire
   - 5.2 Failure of communications services
   - 5.3 Failure of outsourced operations
   - 5.4 Loss or Absence of Key Personnel
   - 5.5 Misrouting/re-routing of messages
   - 5.6 Operational Staff or User Errors
   - 5.7 Software/Programming Errors
   - 5.8 Technical failures
   - 5.9 Transmission errors

Source: Australian TRA standard

Limitations of TRA

- The adversary's SKRAMO is not known
  - Skills
  - Knowledge
  - Resources
  - Authority
  - Motives
  - Objectives

Source: Donn Parker

ROI or subjective decision?

Security Risk	**Business risk**
Involuntary risk of unknown value cannot be avoided	Voluntary discretionary investment decision can be made
Explicit sources of risk are not identifiable	Competitors are known
Adversaries’ skills, knowledge, resources, authority, motives and objectives (SKRAMO) are unknown	Competitors’ SKRAMO is known
Adversaries normally lie, cheat, deceive, and act irrationally	Predictable competitors normally follow ethical practices
ROI is negative, unknown, and not provable: Positive benefit = absence of unknown possible loss Negative result is unlimited, unknown loss	ROI is zero or positive and can be easily demonstrated: Positive benefit is measurable profit Loss is limited to investment
Risk assessment is not verifiable because results are obscure	Risk assessment is verifiable by obvious results
Limited resources are allocated for risk assessment	Generous resources are allocated for risk assessment

-- Donn Parker (with permission)

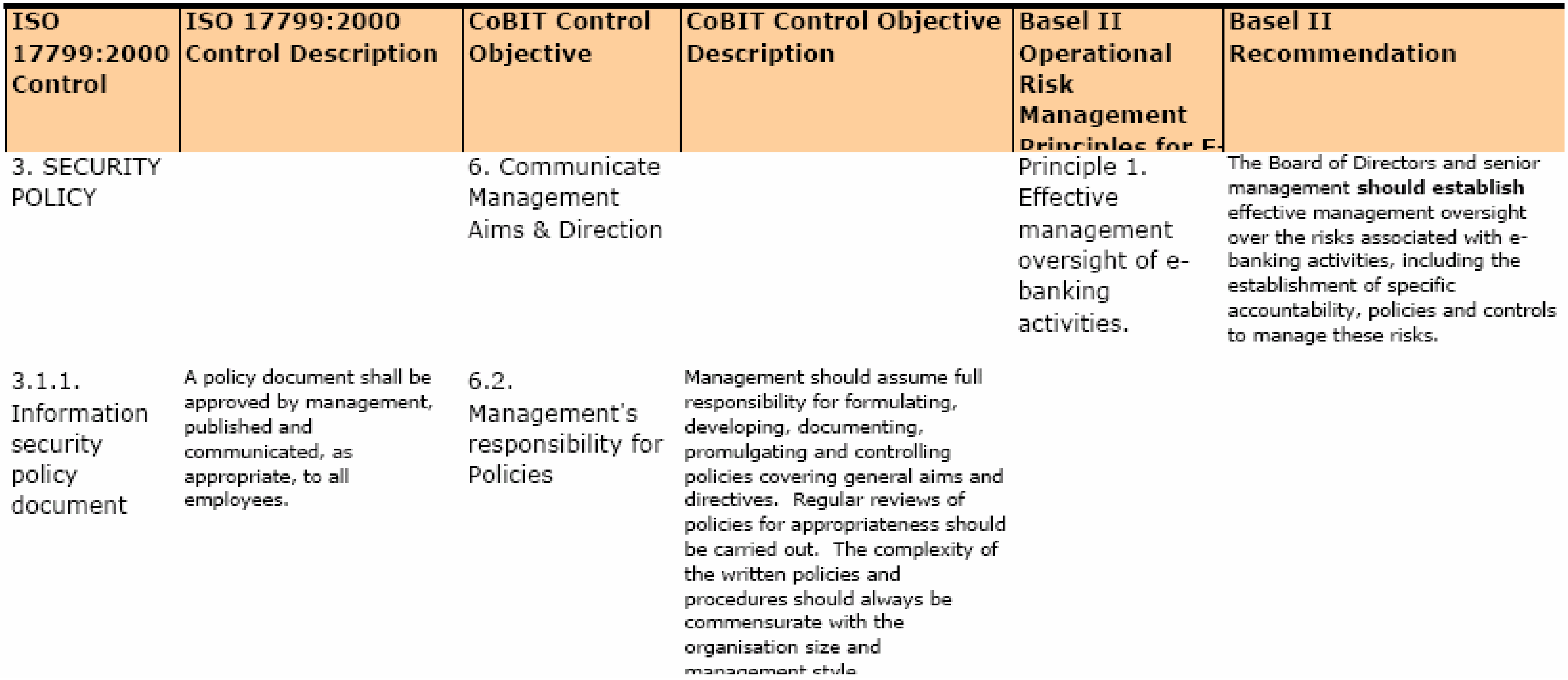
Source: Donn Parker

Security trade-offs are subjective and depend on power and agenda*

That said, you can still appeal to objectivity via benchmarking & principles.

*Source: Bruce Schneier

Gap assessment, standards & benchmarking



ISO 17799:2000 Control	ISO 17799:2000 Control Description	CoBIT Control Objective	CoBIT Control Objective Description	Basel II Operational Risk Management Principles for E-	Basel II Recommendation
3. SECURITY POLICY		6. Communicate Management Aims & Direction		Principle 1. Effective management oversight of e-banking activities.	The Board of Directors and senior management **should establish** effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.
3.1.1. Information security policy document	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	6.2. Management's responsibility for Policies	Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organisation size and management style		

Opportunities to Share or Benchmark

- HTCIA
- Information Security Forum (ISF)
- International Information Integrity Institute (I-4)
- CoBIT Online
- Consulting organizations
- Other fora: FIRST, BITS, etc.

Agenda

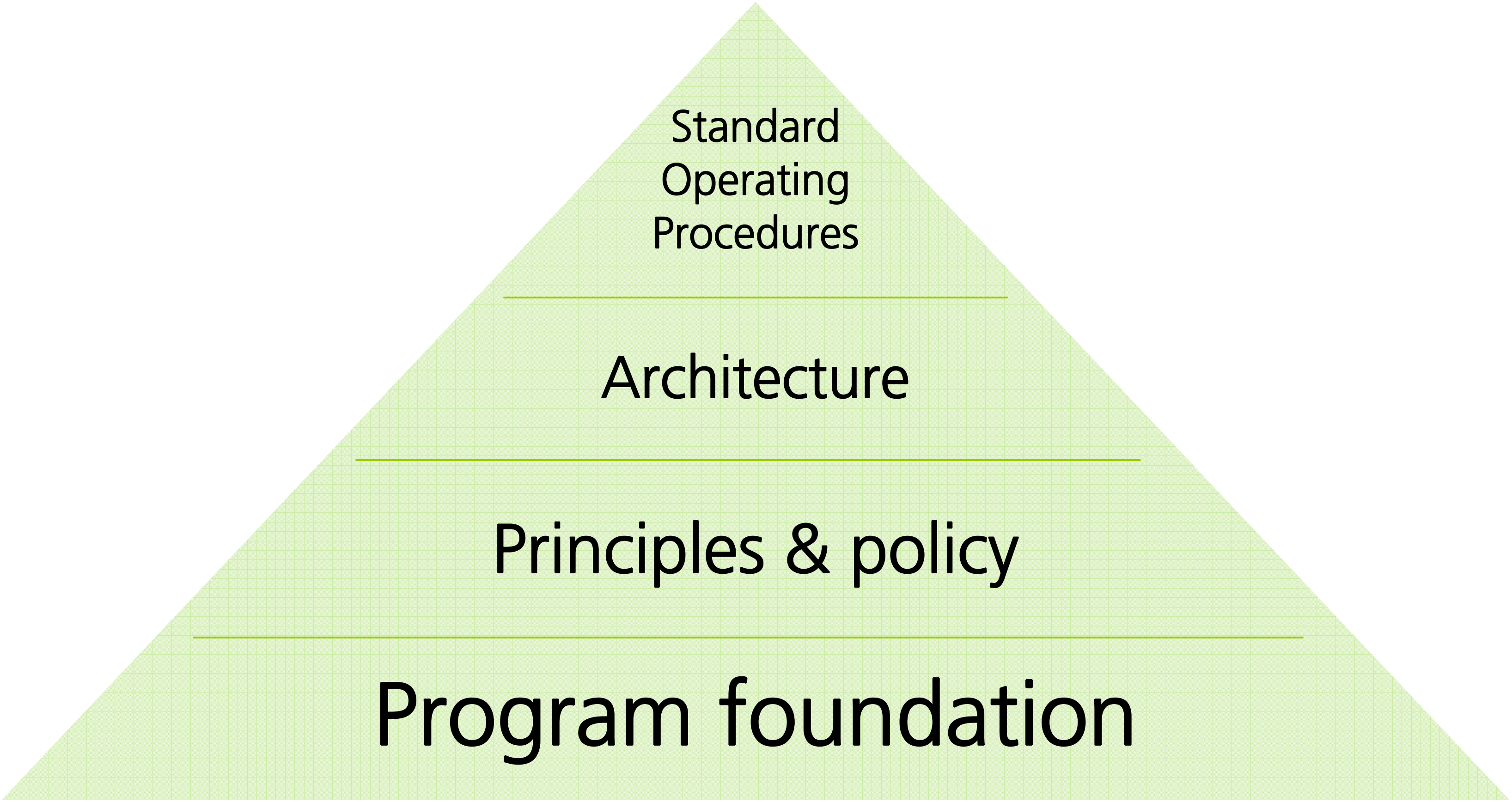
Threats and Risks

Threat-Risk & Gap assessment

Enterprise security architecture

Wireless security architecture

Context of Security Architecture



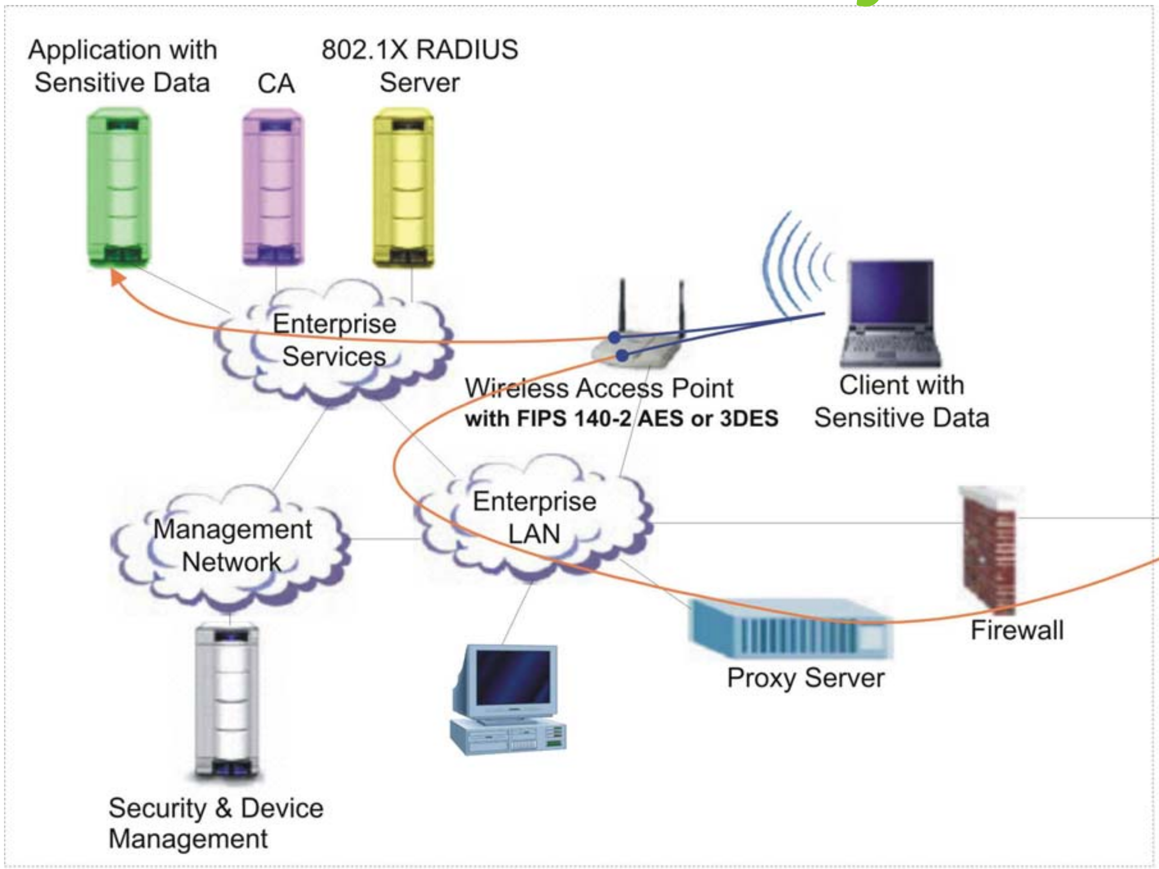
Standard Operating Procedures

Architecture

Principles & policy

Program foundation

A wireless security solution



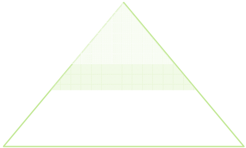
LEGEND

—● Layer 2 AES Encryption (e.g. WPA2 / IEEE 802.11i)

→ Application traffic (unencrypted; or with session-layer encryption via SSL, TLS, SSH, etc)

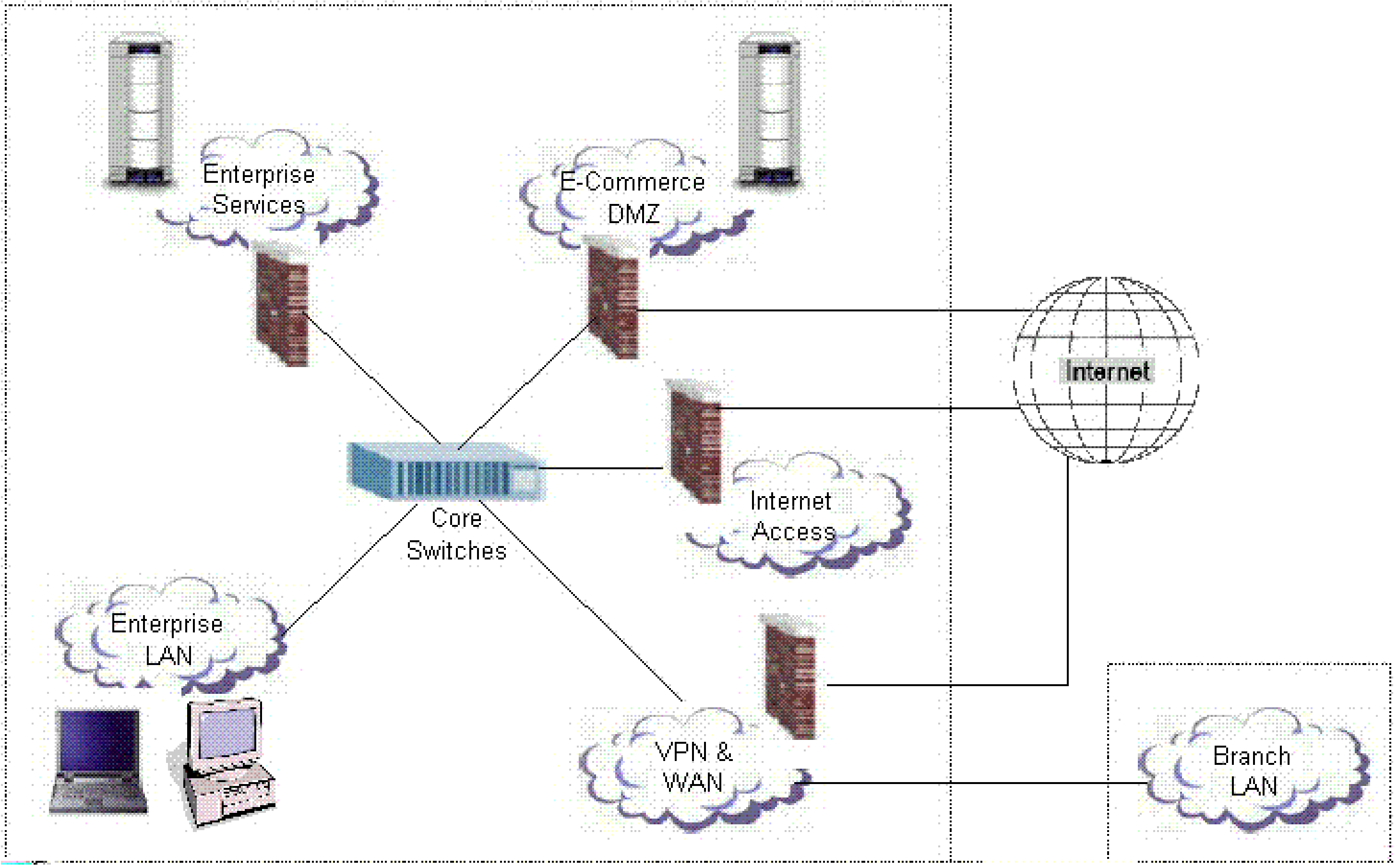
Source: Based on diagrams developed by
Andre Carrington for Center for Internet Security
Wireless Benchmark using DoD graphics

Security Architecture



- Conceptual and functional architecture
  - Services & channels
  - Requirements
  - Decision points
  - Design alternatives & decisions ← Principles
  - Network zones
  - Logical components
  - Object interaction diagrams & state models

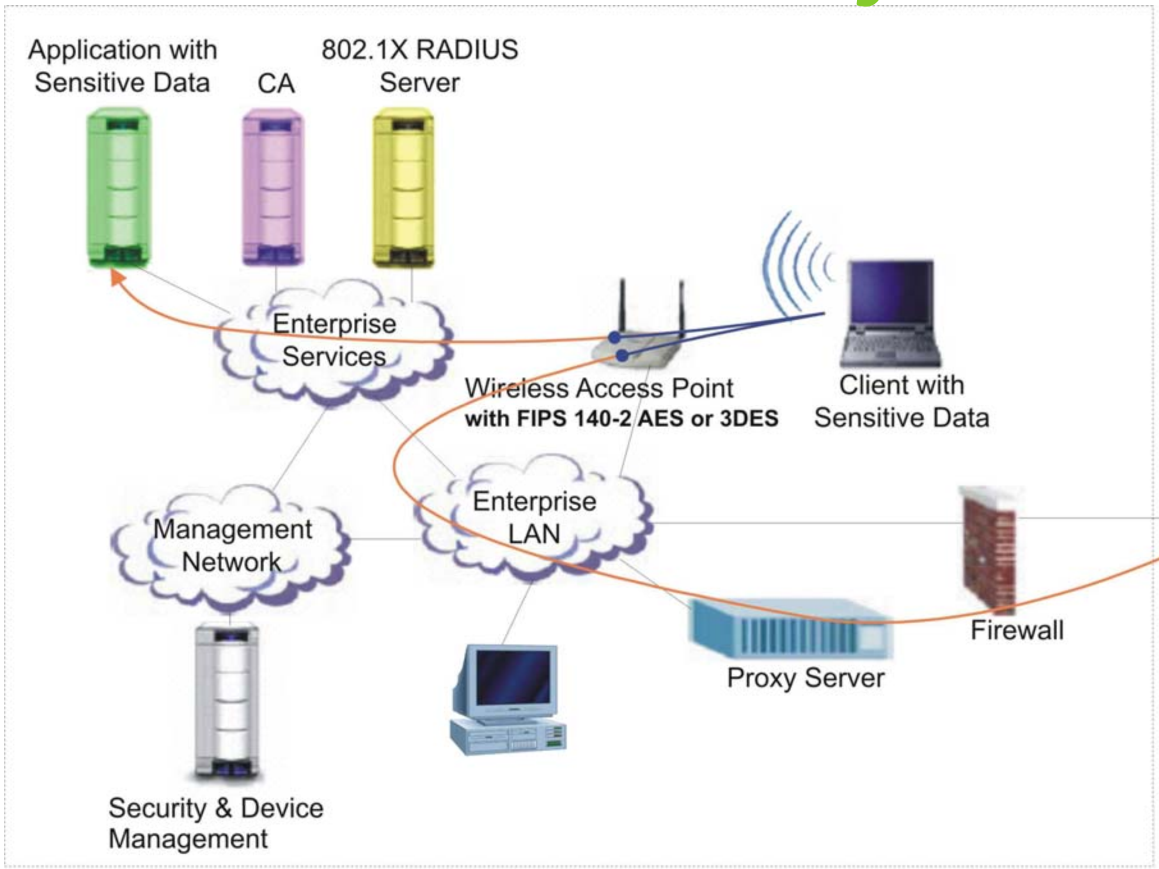
Network Zones



Security Architecture checklist

- Prevent
  - Authorization, Authentication, Access Control, Confidentiality, Audit Logging, System Integrity, Data Integrity and Non-Repudiation
  - Auditing, Ethical Hacking, Compliance Review, Vulnerability Analysis
- Detect
  - Host Intrusion Detection, Network Intrusion Detection, Honey pots/tokens
  - Log Review, Event Correlation, Fraud Detection
- Respond
  - Incident Response, Forensics, Recovery, Duress Alarms, Monitoring
- Enable
  - Role-Based Access Control, Single Sign-On, Provisioning & Identity Management, Digital Signature, Privacy Enhancing Technologies
  - Virtual Private Networking, Secure E-mail, etc.

A wireless security solution



LEGEND

- ●── Layer 2 AES Encryption (e.g. WPA2 / IEEE 802.11i)
- ──► Application traffic (unencrypted; or with session-layer encryption via SSL, TLS, SSH, etc)

Source: Based on diagrams developed by
Andre Carrington for Center for Internet Security
Wireless Benchmark using DoD graphics

Security architecture principles I

- Trade-offs
  - Trade-offs are a part of security design:
    - Cost
    - Time-to-market
    - Performance / Efficiency
    - Usability

- Need to know / Least privilege
  - User groups and privileges
  - ACLs on files, tables, objects, libraries, etc.
  - Firewall & VPN rules (ACLs)
  - Role-based access control

Security architecture principles II

- Weakest link
  - People can be deceived (social engineering)
  - Weak passwords trump strong security
  - Physical access trumps strong logical access controls
  - Avoid non-secure protocols in system administration
    - e.g. telnet, tftp, r-commands, vnc, weak configurations of RDP & X-Windows, etc.
  - Avoid non-secure protocols in untrusted zones
    - ftp, smb, pop3, wep, etc.

- Corollary: Segregate different levels of risk
  - DMZ vs. Internal network
  - Prevent “read-up” and “write-down”
  - Isolate risks / reduce complexity
  - B2C, B2B, Outbound Internet Access, Inbound VPN Access
  - Application tiers: client → web server → integration server → DBMS
  - Separate FTP servers from Web servers

Security architecture principles III

- Keep It Simple (KISS)
  - Simple & specialized components are more secure
  - Reduce, limit and customize: interfaces & services
    - E.g. hardening, stored procedures
  - Avoid infamous services & protocols

- Defense-in-depth / Fail-safe
  - Multiple safeguards of different types:
    - Firewall; Hardening; Logging; File Integrity checking
  - Fail-safe design:
    - DMZ; VLANs that fail-closed; deny-all rules;
    - Non-admin. application users; Chroot/jailed services
    - Database views; session timeout
    - Input validation, buffers, race conditions, infinite loops
    - Stack-heap protection, garbage collection

Security architecture principles IV

- Use Industry Standards, Guidance & Regulations
  - ISO 13335, ISO 7498-2, NIST: SP 800 Series & DISA STIGs
  - VISA & Mastercard PCI Data Security (formerly CISP/SDP)
  - CIS, NSA, IATFF, BITS, etc.
  - ISO 17799, Basel II, SB1386, etc.
  - Vendor guidance
  - Training and Certification
- Obscurity is a weak logical security control

Security architecture principles V

- Built-in not bolted on
- Centralization & Automation
  - Logging, Intrusion Detection & Event Management
  - Authentication servers for users & devices
  - Centralized User Administration / Single Sign On (to some extent)
  - Vulnerability assessment & reporting

Agenda

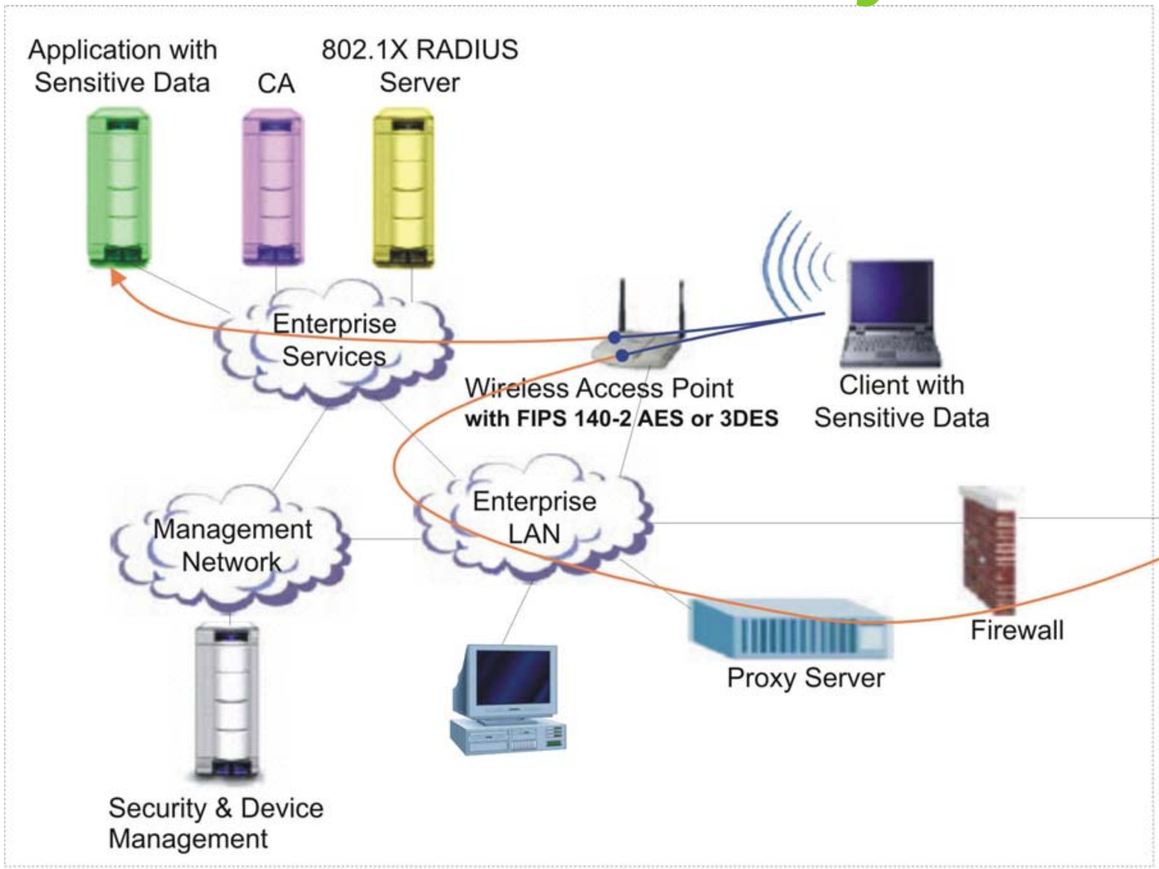
Threats and risks

Threat-Risk & Gap assessment

Enterprise security architecture

Wireless security architecture

A wireless security solution



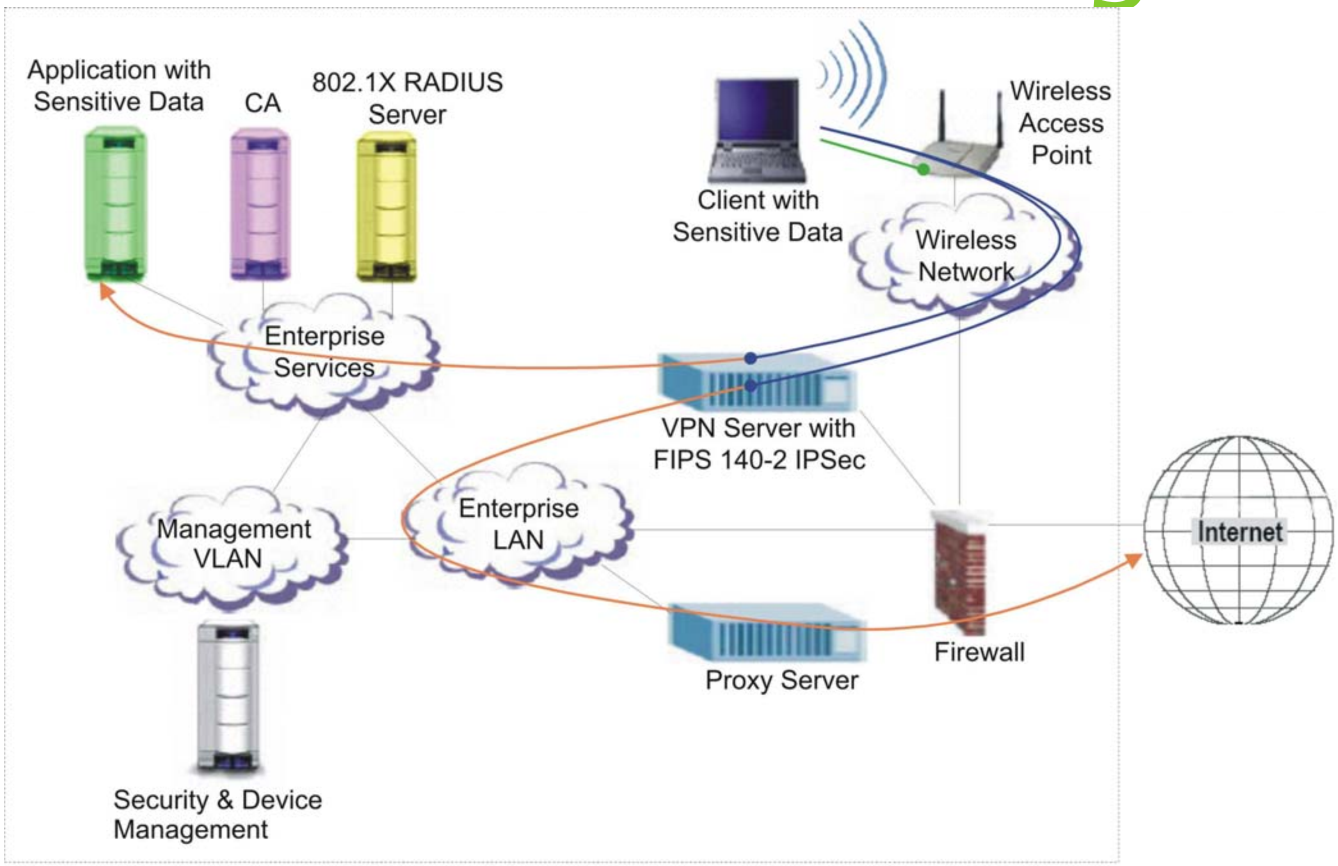
LEGEND

—● Layer 2 AES Encryption (e.g. WPA2 / IEEE 802.11i)

→ Application traffic (unencrypted; or with session-layer encryption via SSL, TLS, SSH, etc)

Source: Based on diagrams developed by
Andre Carrington for Center for Internet Security
Wireless Benchmark using DoD graphics

Is this a better design?

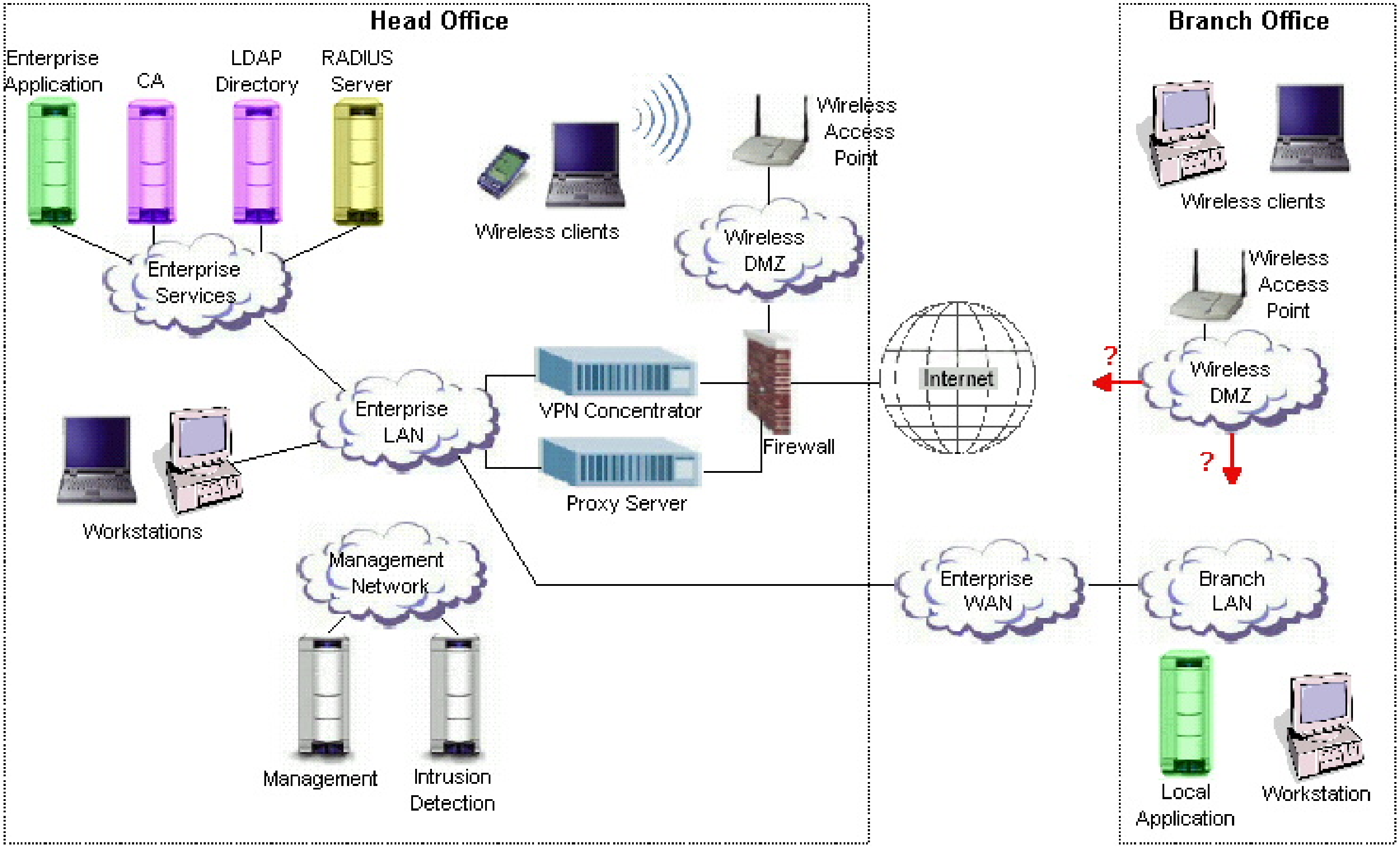


LEGEND

- —● Layer 3 FIPS 140-2 IPSec with AES or 3DES Encryption
- —▶ Application traffic (unencrypted; or with session-layer encryption via SSL, TLS, SSH, etc)
- —● Optional Layer 2 AES or 3DES Encryption

Source: Based on diagrams developed by
Andre Carrington for Center for Internet Security
Wireless Benchmark using DoD graphics

Scalability?



Source: Based on diagrams developed by
Andre Carrington for Center for Internet Security
Wireless Benchmark using DoD graphics

Thank-you for your time.

Profile

Mr. Carrington is a consultant with 13 years of professional experience in IT security and e-business integration. He has devised security architectures, performed risk assessments and developed e-commerce applications for banks, insurance companies and other private and public sector organizations.

Mr. Carrington is a systems design engineer from the University of Waterloo, a Certified Information Systems Security Professional and a Certified Information Security Manager. He has secret (level II) clearance with the Government of Canada.