

Privacy, Security & Ethics for CS 792 Health Informatics I Data Structures & Standards

WATERLOO
CHERITON SCHOOL OF
COMPUTER SCIENCE

cs.uwaterloo.ca

André M. Carrington
P.Eng, CISSP, CISM, CISA, CIPP/C

my academic background

Undergrad:
Systems
Design
Engineering

URA:
Optometry



Masters
of Health
Informatics
(near completion)

<http://www.bedrocksecurity.com/academic.html>

André M. Carrington

employment



André M. Carrington

WATERLOO | CHERITON SCHOOL OF COMPUTER SCIENCE

clients



Preface

- To think like a privacy and security specialist
- Models are not exact but useful
- The Pragmatist vs. the Purist
 - Seek agreement on higher-level principles first vs. detailed requirements, to avoid getting stuck
 - Don't worry about strict adherence to any one method
 - Disagreement about requirements, may be a timing issue re budget, availability of resources, etc. Agree on the roadmap.

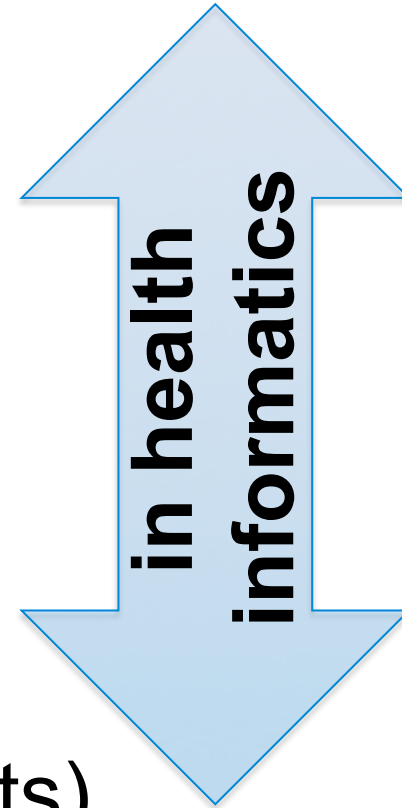
Agenda

privacy & security

- concepts
- architecture
- detailed design

ethics

trends (if time permits)



Privacy concepts



"On the Internet, nobody knows you're a dog."

André M. Carrington

WATERLOO | CHERITON SCHOOL OF COMPUTER SCIENCE

Does privacy matter to you?

What is privacy about?

-
-
-
-
-
-
-

Key expressions of privacy

- **“right to be let alone”**
 - Warren & Brandeis, 1890
 - Katz v. United States (supreme court re 4th amendment), 1967

- **“No one shall be subjected to arbitrary interference with his **privacy, family, home or correspondence**, nor to attacks upon his **honor and reputation**”**
 - U.N. Universal Declaration of Human Rights, 1948

Key expressions of privacy

- “Everyone has the right to **respect** for his private and family life, his **home** and his **correspondence**”
 - European Convention of Human Rights, 1950
- “We protect privacy when we consider the **dignity** of individuals about whom we know things, and when we use what we know about them only in ways which **preserve** and enhance that **dignity**.”
 - Burton Group’s Golden Rule
Identity and Privacy Strategies: Privacy

Privacy (and security) may relate to your:

- body, dna
- home, property
- personal activities
- personal information (& communications)

Which of these are sensitive?

- name, home address, phone number, social insurance number, health card number, credit card number, age, sex, postal code

Which of these are sensitive?

- name, home address, phone number, social insurance number, health card number, credit card number, age, sex, postal code
- mental illness, communicable disease, disabilities, abortion, sexual dysfunction, infertility, physical abuse, sexual abuse

Which of these are sensitive?

- name, home address, phone number, social insurance number, health card number, credit card number, age, sex, postal code
- mental illness, communicable disease, disabilities, abortion, sexual dysfunction, infertility, physical abuse, sexual abuse
- any health data

Which of these are sensitive?

- name, home address, phone number, social insurance number, health card number, credit card number, age, sex, postal code
- mental illness, communicable disease, disabilities, abortion, sexual dysfunction, infertility, physical abuse, sexual abuse
- any health data
- current & past location, numbers called, websites visited, transactions, source ip address, OS & browser fingerprints

Some people are more private than others – privacy is in the eye of the beholder (data subject)



Personal health information

“The Ontario government has some of the strictest privacy protection in the world.

It's something we're building into our...services... particularly when it comes to **health records, which are the most sensitive and personal information we handle**, as a government.”

- Ontario Premier Dalton McGuinty

Definition of PI

- ‘ “personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.’ -- PIPEDA
- PI **excludes** data that is **not individually identifiable**, e.g. cell size (or k-anonymity) where $k > 5$
-- IPC Ontario orders, MOHLTC policy
- PI **includes** a Business E-mail Address!
unless it is “publicly available” for the purpose of collection, use...
-- Privacy Commissioner of Canada

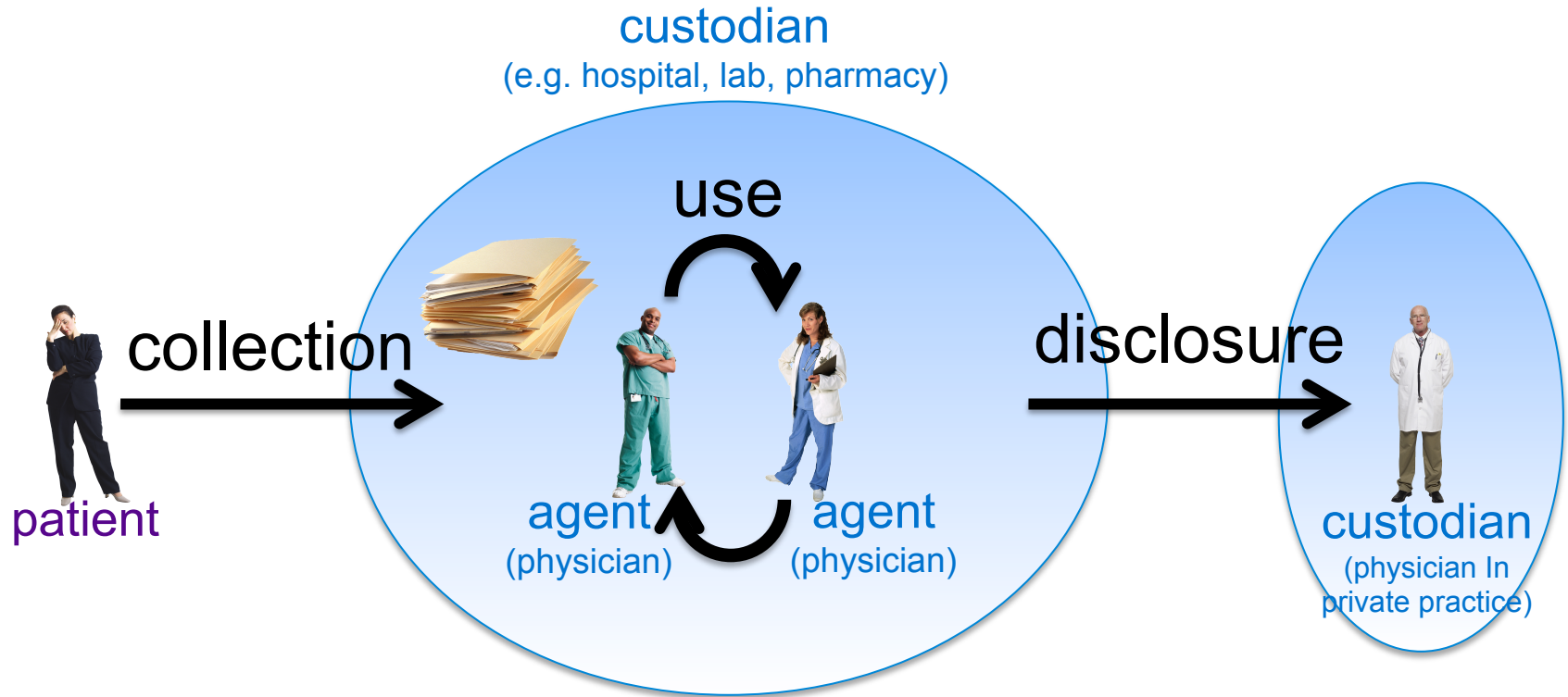
Definition of PHI (paraphrased)

“personal health information”, with respect to an individual, whether living or deceased, means

- info re physical or mental health
 - info re any health service provided
 - donation of any body part or bodily substance, or info derived therefrom
 - info collected while providing health services
 - info collected incidentally while providing health services
- paraphrased from PIPEDA

Information Privacy is about C.U.D.

collection, use & disclosure of personal information



The 10 principles in the CSA Model Code of Privacy

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use,
Disclosure, Retention ...and more...

What are the risks?



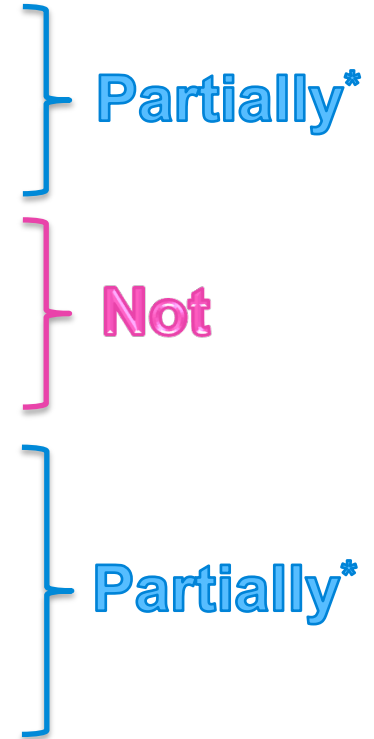
André M. Carrington

The 10 principles in the CSA Model Code of Privacy

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Some ideals are partially coded, or not encoded, in health/privacy laws

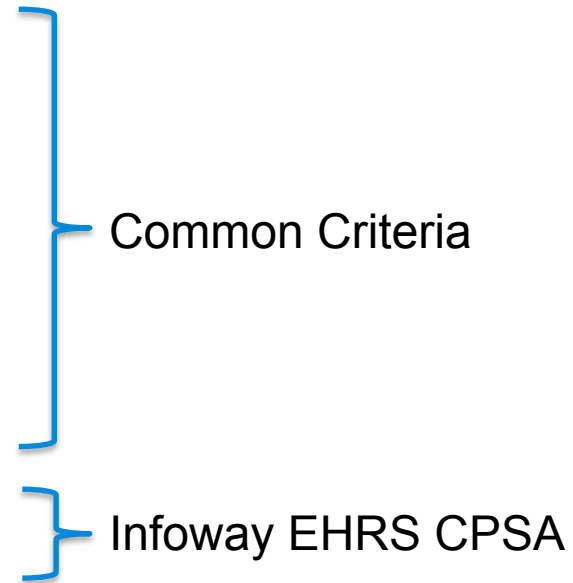
- Control (of use & disclosure)
= Informational self-determination
- Limiting purpose
- Legitimacy of purpose
- The 4 common criteria requirements...
- Breach notification
- Penalties



*Perhaps minimally

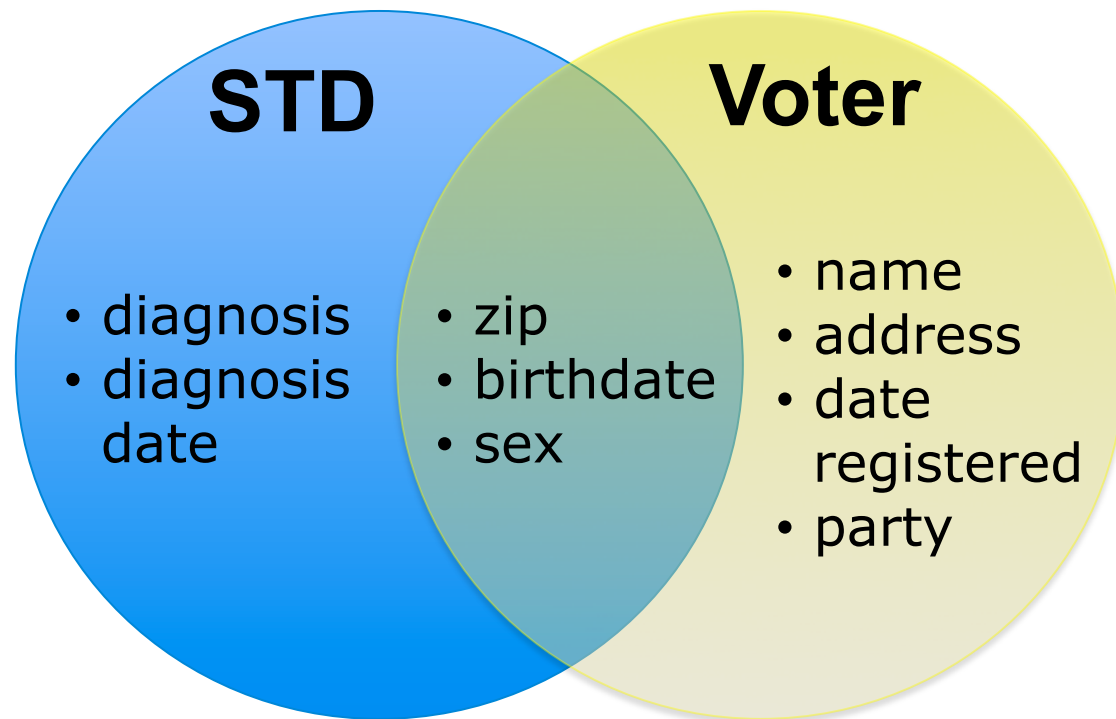
Atomic and unique functional & technical privacy requirements

- Anonymity
- Pseudonymity
- Unlinkability
- Unobservability
- Consent Directives



A simple re-identification example from Ochoa et al.

*conceptual
data model*



Combining the de-identified STD database with identifiable voter data

Deidentified Database

Control Database

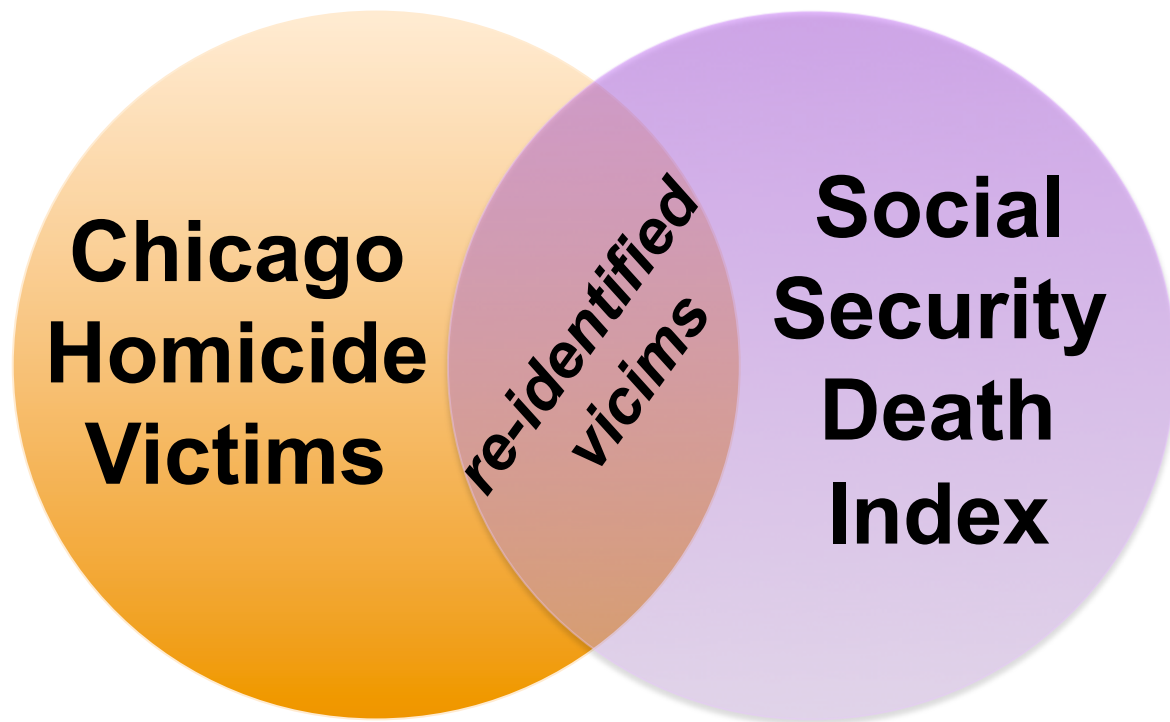
Subject	Personal Information	Shared Quasi-identifier {ZIP, birth date, sex}	Name	Street Address	Party Affiliation
1	Illness 12	{02139, 08/28/52, M}	Bill Robinson	1 Main Street	Democrat
2	Illness 1	{02139, 02/14/62, F}	Marsha Wilkins	15 Broadway	Republican
...

Identifiers

- **Explicit-identifiers** *individually* identify some persons within a population
 - name, address, phone number, social insurance number, health card number, credit card number
- **Quasi-identifiers** *in combination*, identify some persons within a population
 - age, sex, postal code; conditions

Ochoa et al.'s paper re-identified 35% of victims by linking two databases

*population
content
view*



Re-identification

Personal Health Information (PHI)

- explicit identifiers
- quasi-identifiers
- data



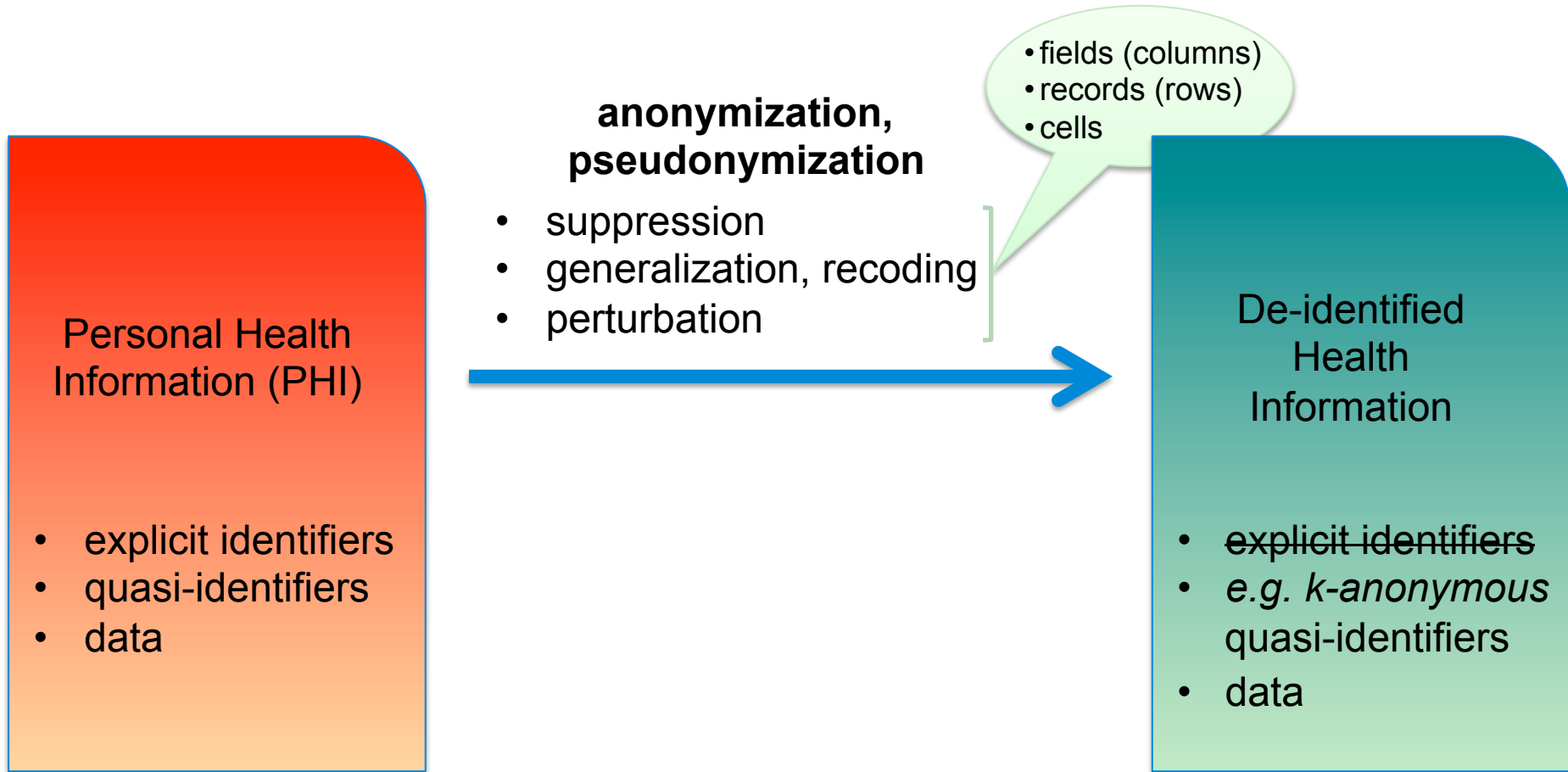
- linking to identifiable/control data
- linking tables, records, across time
- statistical inference
- outliers

- areas
- groups
- individuals

De-identified Health Information

- explicit identifiers
- e.g. *k-anonymous* quasi-identifiers
- data

De-identification



Standards, Laws and Policies

De-identification...

- ISO 25237 Pseudonymization
- CIHI HSU working group - Best Practice Guidelines for Managing the Disclosure of De-Identified Health Information
- US HIPAA
- ASTM International VUHID Standards

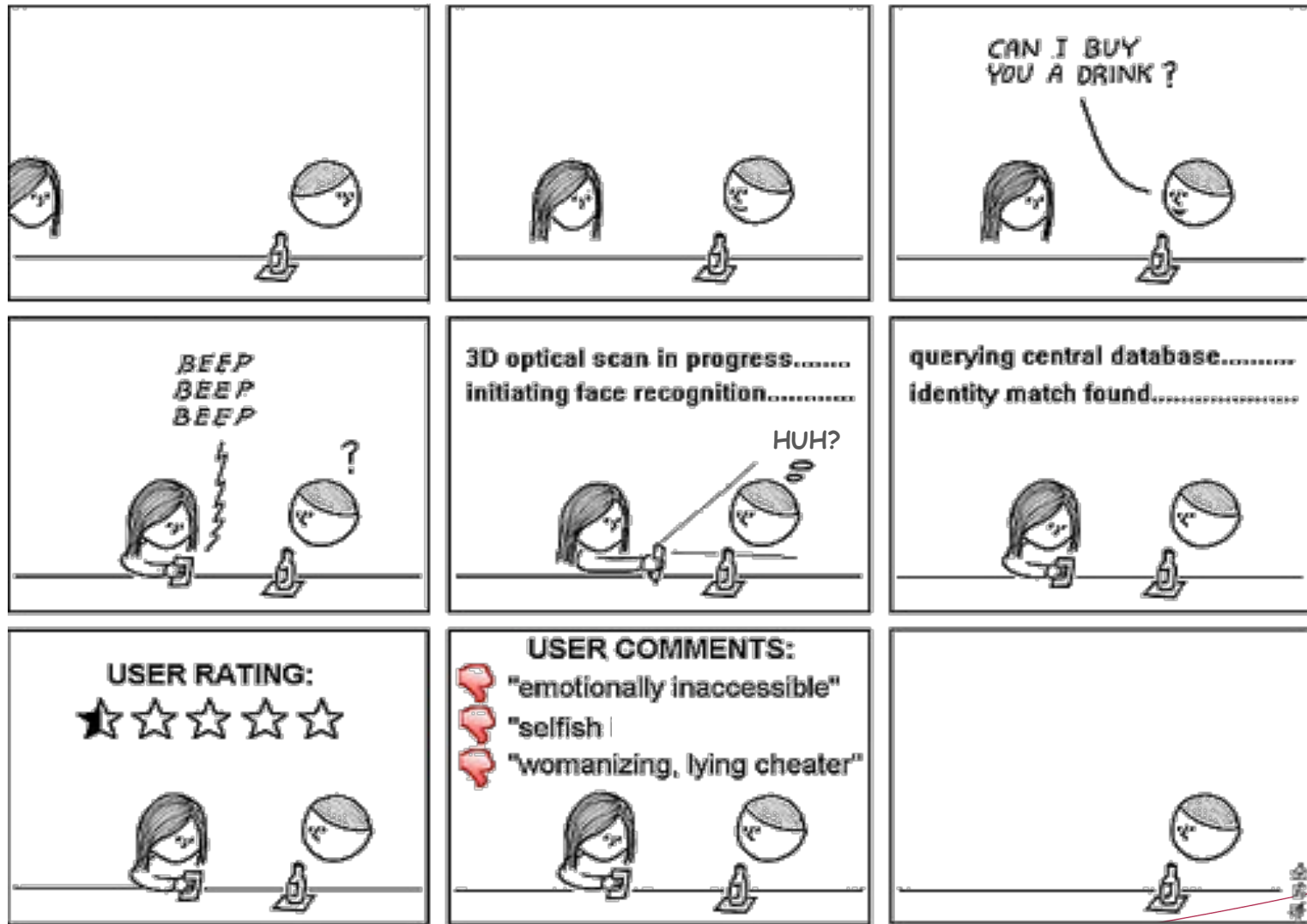
...and Disclosure Control

- Census Canada on Uniqueness
- Canada Post on FSAs
- ON MOHLTC Policy on Cell Sizes
- Privacy Commissioners (Fed, ON, BC) on thresholds of identifiability
- UNECE Managing Statistical Confidentiality & Microdata Access

Some Tools

- Canada
 - PARAT (El Emam)
 - REB & IRB Wizards (El Emam)
 - Camouflage
 - US
 - Privacert Appliance (Sweeney): HIPAA certified
 - Datafly and k-similar (Sweeney)
 - VUHID service
 - Europe
 - μ -Argus and τ -Argus
- etc.

Personal C.U.D. is not covered



André M. Carrington

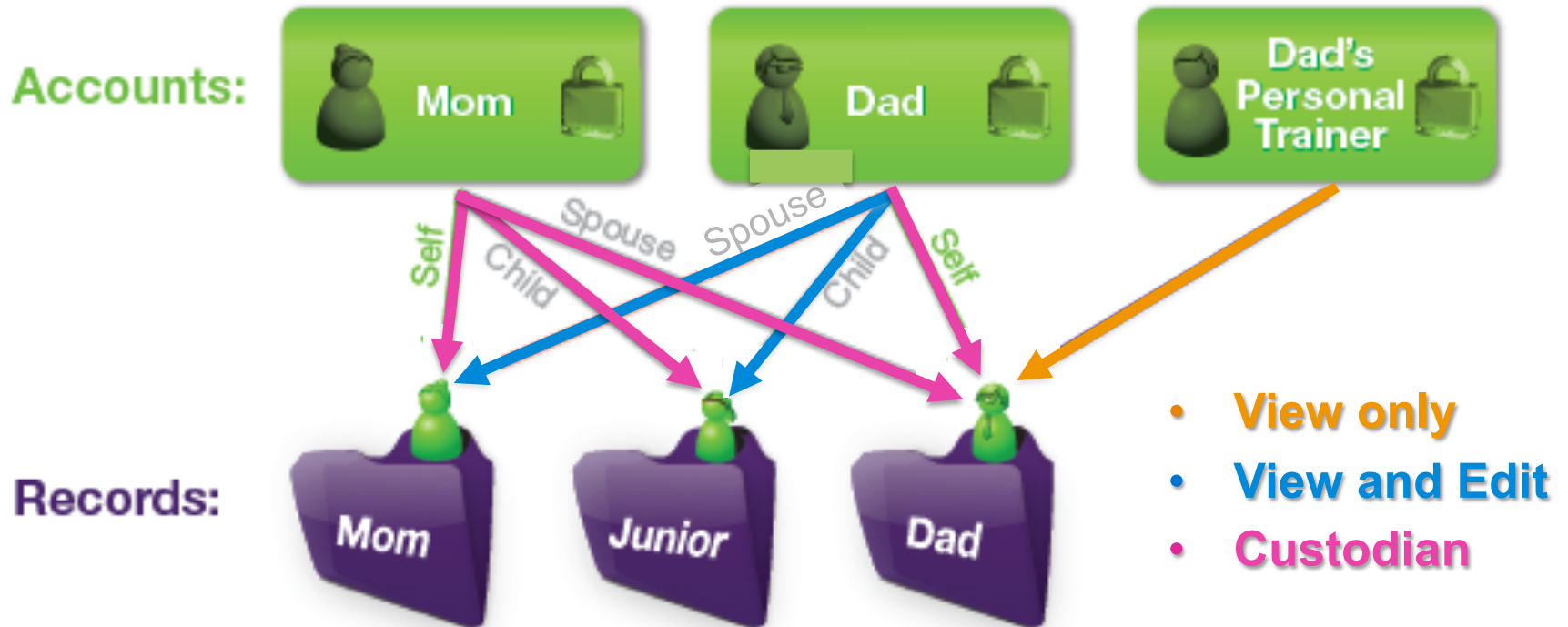
Personally-controlled health records have 1 or more family members as custodians



André M. Carrington

WATERLOO | CHERITON SCHOOL OF COMPUTER SCIENCE

Example of Microsoft Healthvault



5 mins: read handout

+ 5 mins: break

video & discussion

thebroken episode 3 - 17:30-20:52

interview with kevin mitnick on identity theft & the SSDI

Alternatively:

<http://www.youtube.com/watch?v=IJFCbrhLojA>

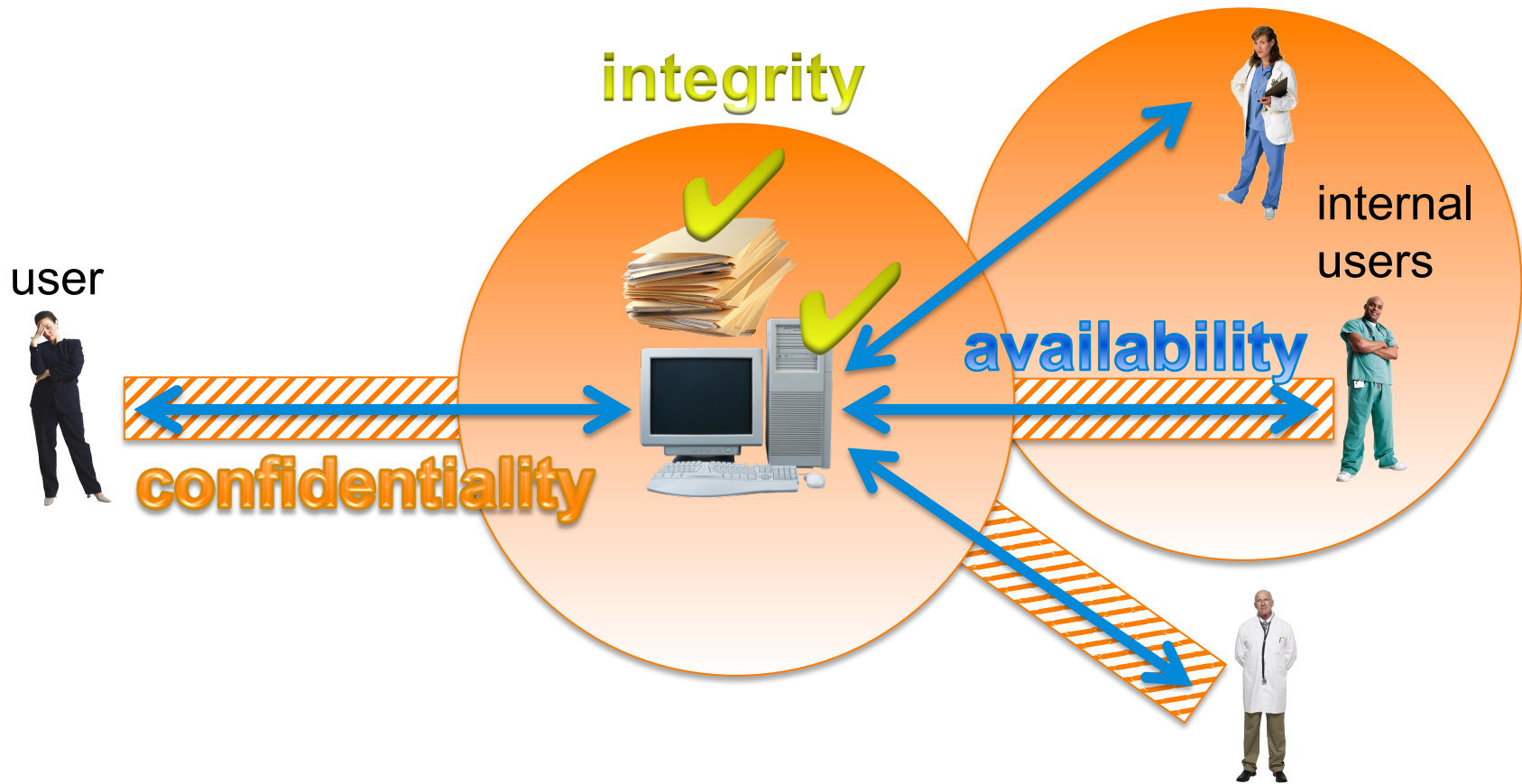
<http://www.youtube.com/watch?v=DqJhg7dOc-g>

Security concepts






André M. Carrington

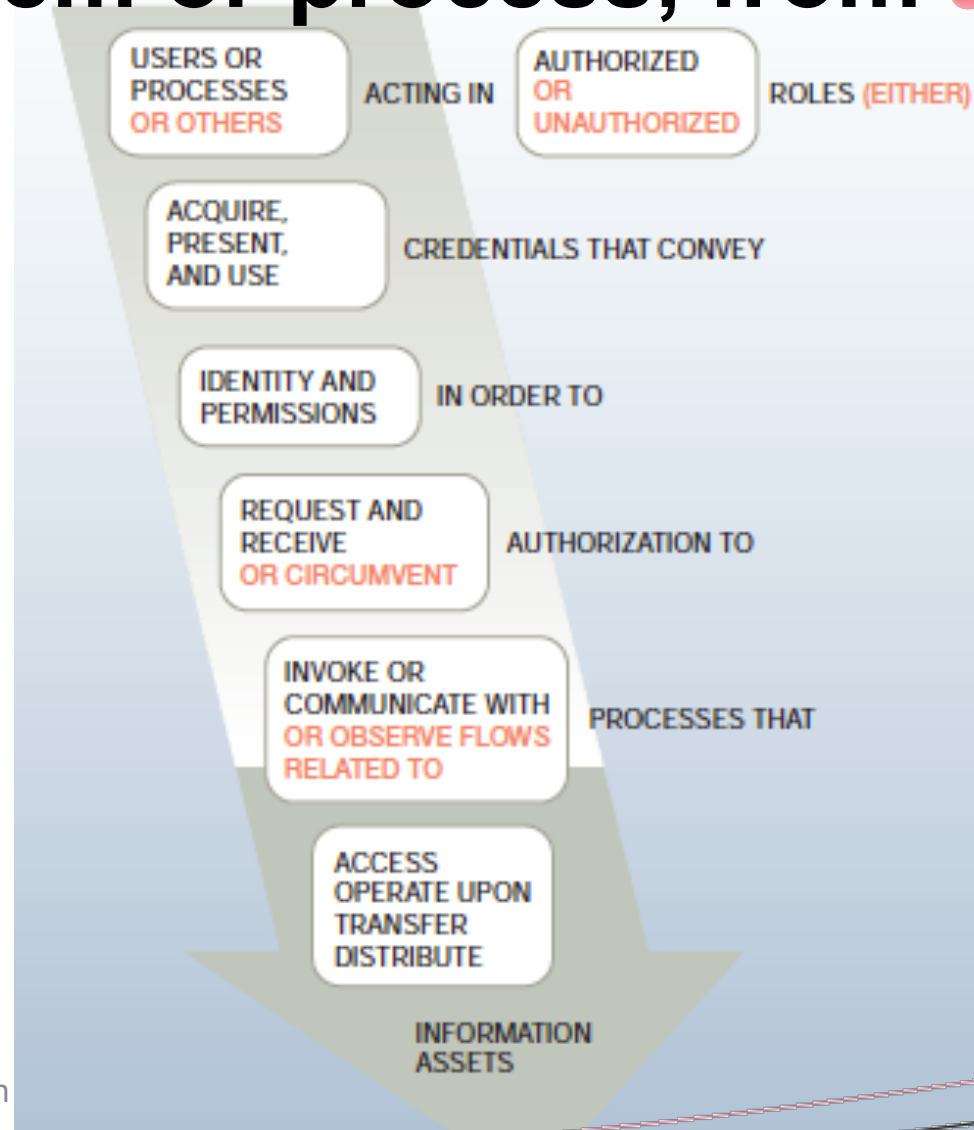
Information Security is about C.I.A. the confidentiality, integrity & availability of data & systems



Security practitioners *may not* cover some aspects of Availability

- accidents or natural events
 - power, fire, flood, pandemic flu, planes & cars
- business continuity planning (BCP)  specialty
- disaster recovery planning (DRP)  specialty
- physical security  specialty
 - e.g. external & internal physical attack, duress

Security protects the normal flow of a system or process, from **attack**



Source: Whitmore, J.J.
A Method for Designing
Secure Solutions

We can enumerate & analyze threats

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: New South Wales Infosec Guide, 2007

But the SKRAMO of a malicious threat agent is not predictable.

Skills

Knowledge

Resources

Authority

Motives

Objectives

-- Donn Parker, top computer crime expert, ACM Fellow, Author
(interviewed more than 200 perpetrators and their victims)

Threat-Risk Assessment has challenges

- Lacks data
- Requires business *and* technical expertise
- Subjective
- Rare (black swan) events are problematic
- Reputation loss & impact difficult to estimate

Code of Practice for Infosec Management – ISO 27002 & 27799

- Policy
 - Committees, roles & responsibilities
 - Assets
 - Human resources
 - Physical security
 - Communications
- ...and more...

Code of Practice for Infosec Management – ISO 27002 & 27799

- Policy
- Committees, roles & responsibilities
- Assets
- Human resources
- Physical security
- Communications
- Access control
- System development & maintenance
- Incidents
- Business continuity
- Compliance

Passwords

- Are often weak, but they will be with us forever!
- Sticky notes
- Shoulder surfing
- Same across sites
- Horizontal attacks
- Predictability (including l33t speak)
- Dictionary and rainbow hash table attacks
- In service-service authentication

3 mins: video

thebroken episode 3 -- 2:20-4:55
physical access, ntpasswd, NTLM hash & LMhash,
Sam Inside & Lophtcrack

A facebook enhancement to reduce unauthorized access.



Please confirm your identity

In order to proceed, Facebook needs to verify that you are the owner of this account. To do this, please identify the people tagged in the following series of photos.

To pass, you cannot get any answers wrong. If you aren't sure about a question, please skip it. You can only skip 2 questions.

Start

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Security risk vs. business risk (ROI)

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' SKRAMO is 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, 2005)

Agenda

privacy & security

- concepts
- **architecture**
- detailed design

ethics

trends (if time permits)

A misconception

- Sometimes I hear folks say that a ***specific*** security service, control or mechanism is required when only a ***general requirement*** is stated
- These are open to interpretation
 - e.g. confidentiality in storage and transmission does not ***require*** encryption except in untrusted zones
 - e.g. high assurance, non-repudiation, digital signature

Privacy & Security objectives

- Manage risk to patients and organizations
- Comply with laws, regulations & precedents
- “ “ commissioner orders
- Meet due care (an implicit legal obligation)
- “ policies, contracts & operating rules
- Enable business (access & interoperability)
- Engender trust

Privacy & Security differences

- Privacy pertains to *personal information and the law*;
- Security pertains to *any asset* and has very few specific requirements in the law

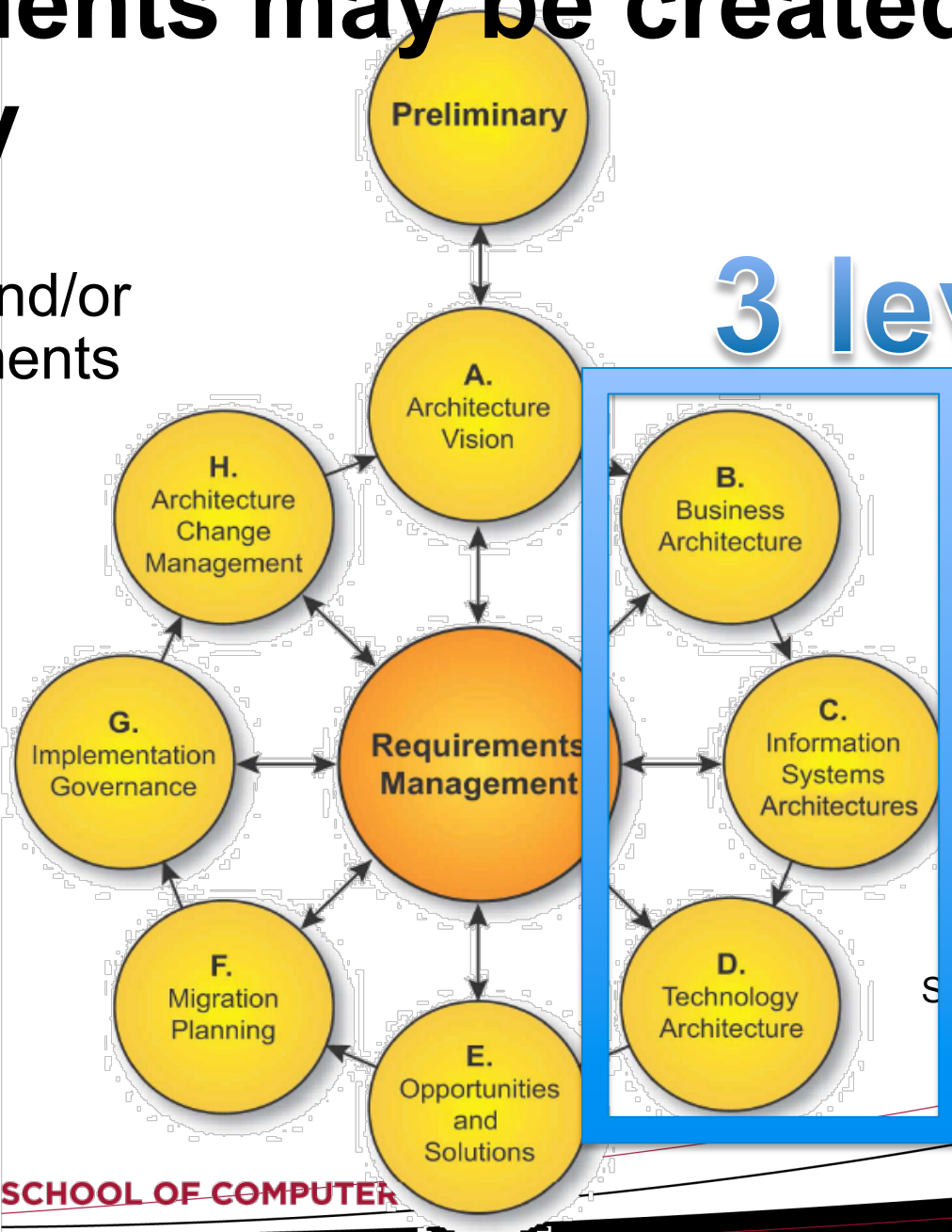
Exercise

- You've joined a big consulting firm.
- You must visit a client, a large corporation with headquarters in Montreal, to review the privacy and security **requirements** that were recently completed for a solution. They will soon be audited by a third party.
- What types of requirements should you find? What documents (as a primary source) should they have used?

Requirements may be created iteratively

complimenting and/or refining requirements from prior steps

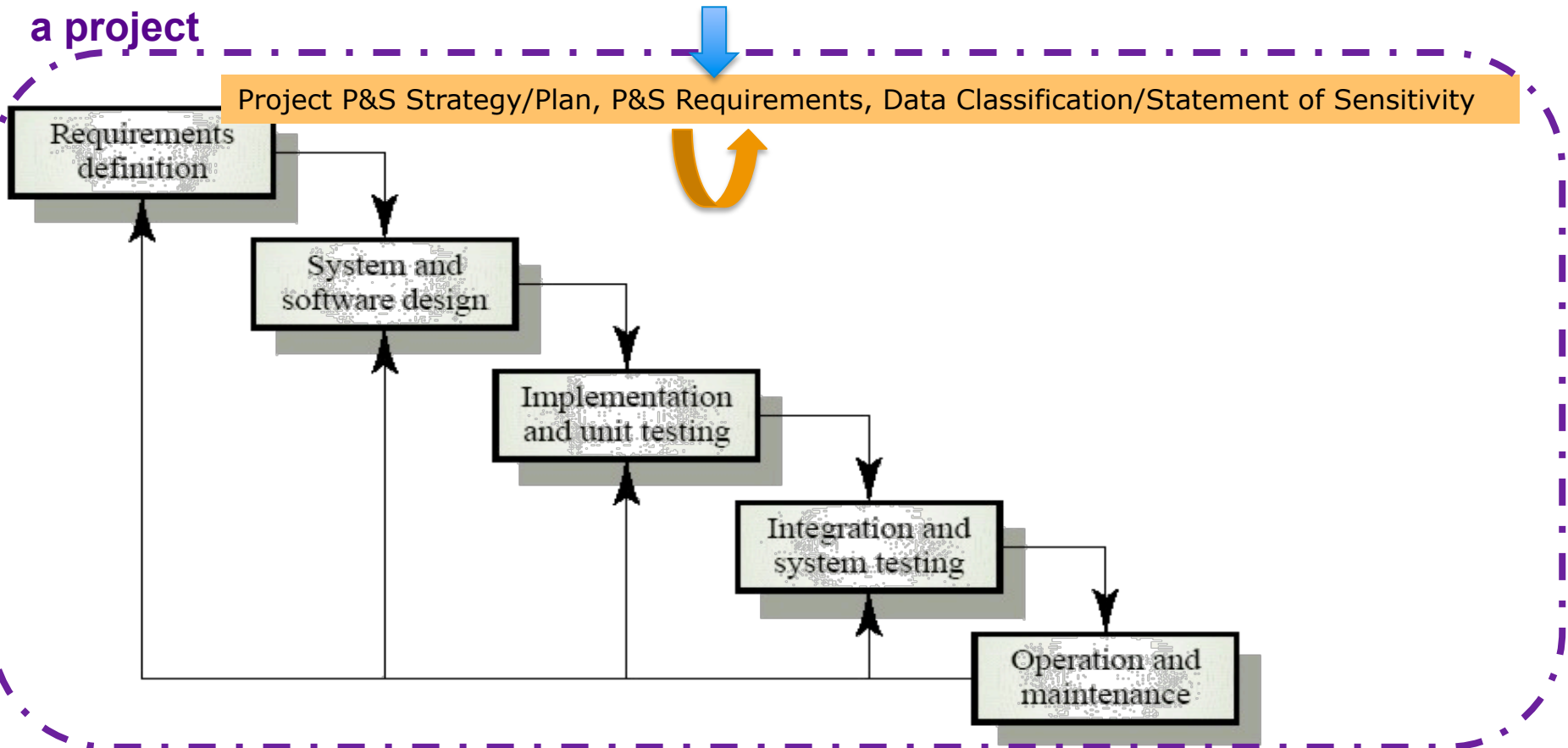
3 levels



Source: TOGAF

Privacy & Security in the Solution Design Life Cycle

a project



Source: ISO 12207

Privacy & Security in the Solution Design Life Cycle

Enterprise-level P&S requirements (i.e. from governance)...

Committees/REBs/IRBs, Working Groups, Roles & Responsibilities, Laws & Regulations, Principles, Policy, Strategy/Budget/Plans, Enterprise Architecture/Frameworks, MOUs/Contracts/SLAs, DSAs/ISAs, Standards, Procedures, Risk Management

Project P&S Strategy/Plan, P&S Requirements, Data Classification/Statement of Sensitivity

Conceptual, Logical and Physical:

Architecture, Privacy Impact Assessment, Threat Risk Assessment Review, Risk Log & Treatment Plan

Development, Configuration, Hardening, Review & Testing Static & Dynamic Analysis, Vulnerability Assessment (VA)

Security Quality Assurance, Certification & Accreditation, Penetration Testing, VA

Penetration Testing, VA Awareness Training Patch Management, Helpdesk Procedures, Audit, Review Change Management Incident Response

Requirements definition

System and software design

Implementation and unit testing

Integration and system testing

Operation and maintenance

André M. Carrington

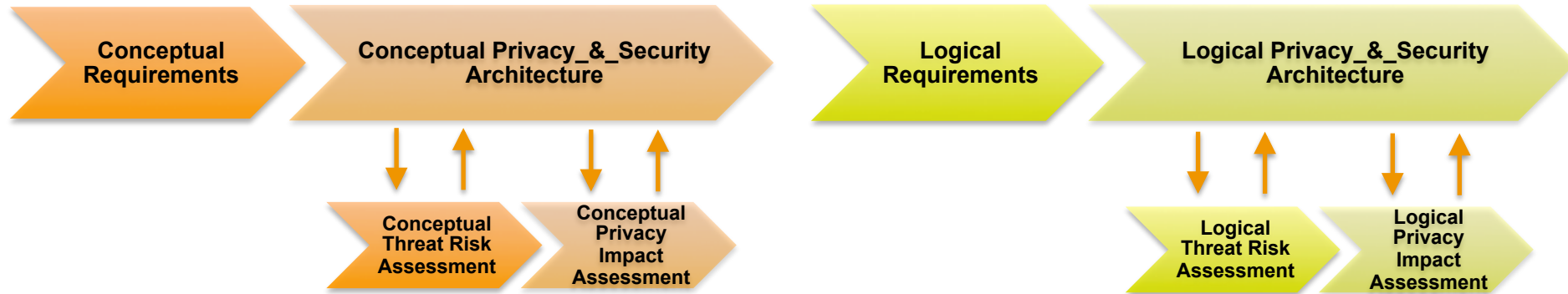
Lifecycles

- Enterprise Architecture (EA)

- Solution Design Life Cycle (SDLC)

- Other:
 - Incident Response
 - Risk Management
 - etc. (*see ITIL*)

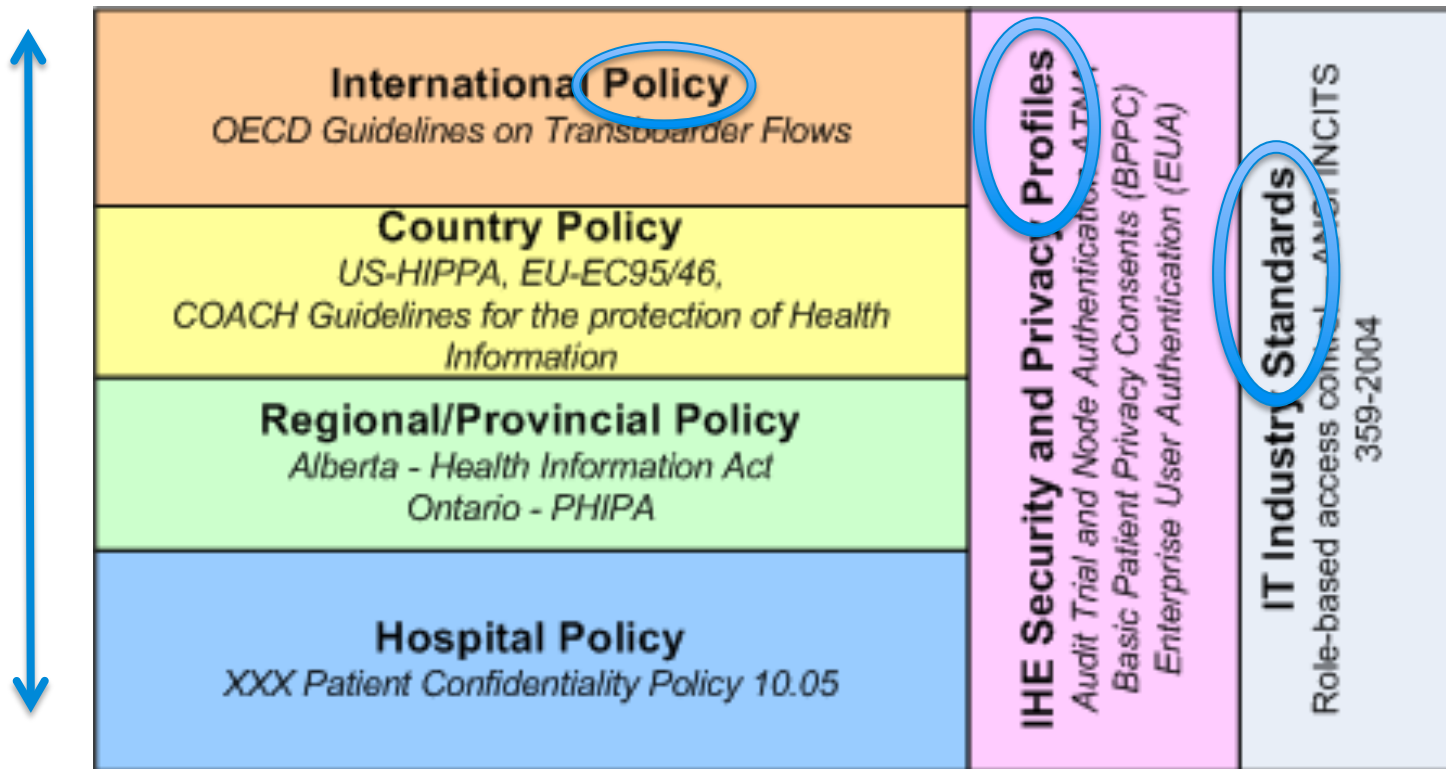
Recommendations from Threat-Risk Assessment also become requirements



TRAs & PIAs have two competing purposes

1. To identify and assess risks – from a complete understanding of the solution.
(PSA starts first, front-loaded)
2. To drive requirements into the solution from TRA and PIA recommendations.
(PSA finishes last)

Patient Information Protection Policies



Laws, Policies & Standards

Level of Jurisdiction

- Provincial, Federal, Municipal
- Regional, International
- Hospital, Org

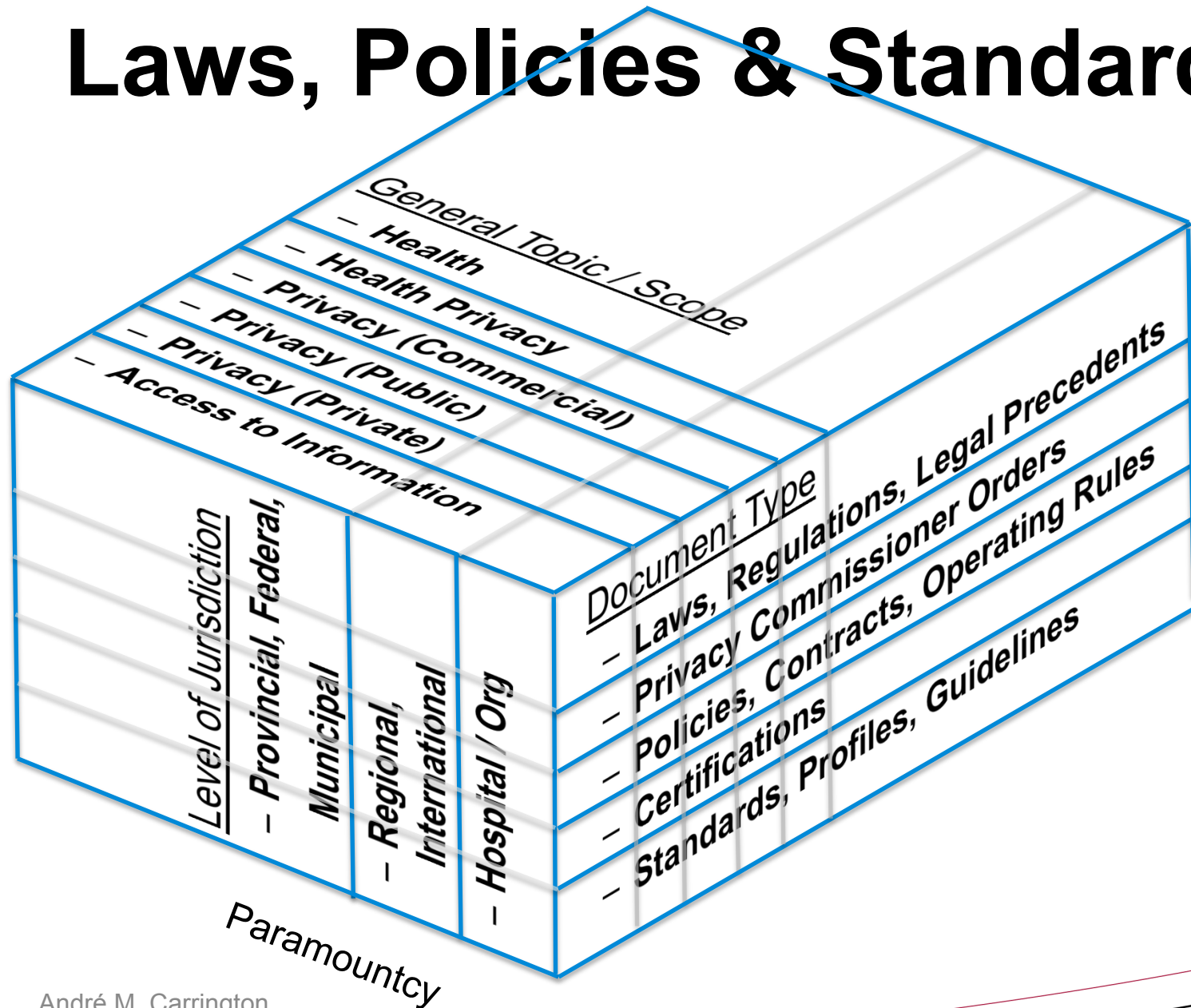
General Topic / Scope

- Health
- Health Privacy
- Privacy (Commercial)
- Privacy (Public)
- Privacy (Private)
- Access to Information

Document Type

- Laws, Regulations, Legal Precedents
- Privacy Commissioner Orders
- Policies, Contracts, Operating Rules
- Certifications
- Standards, Profiles, Guidelines

Laws, Policies & Standards



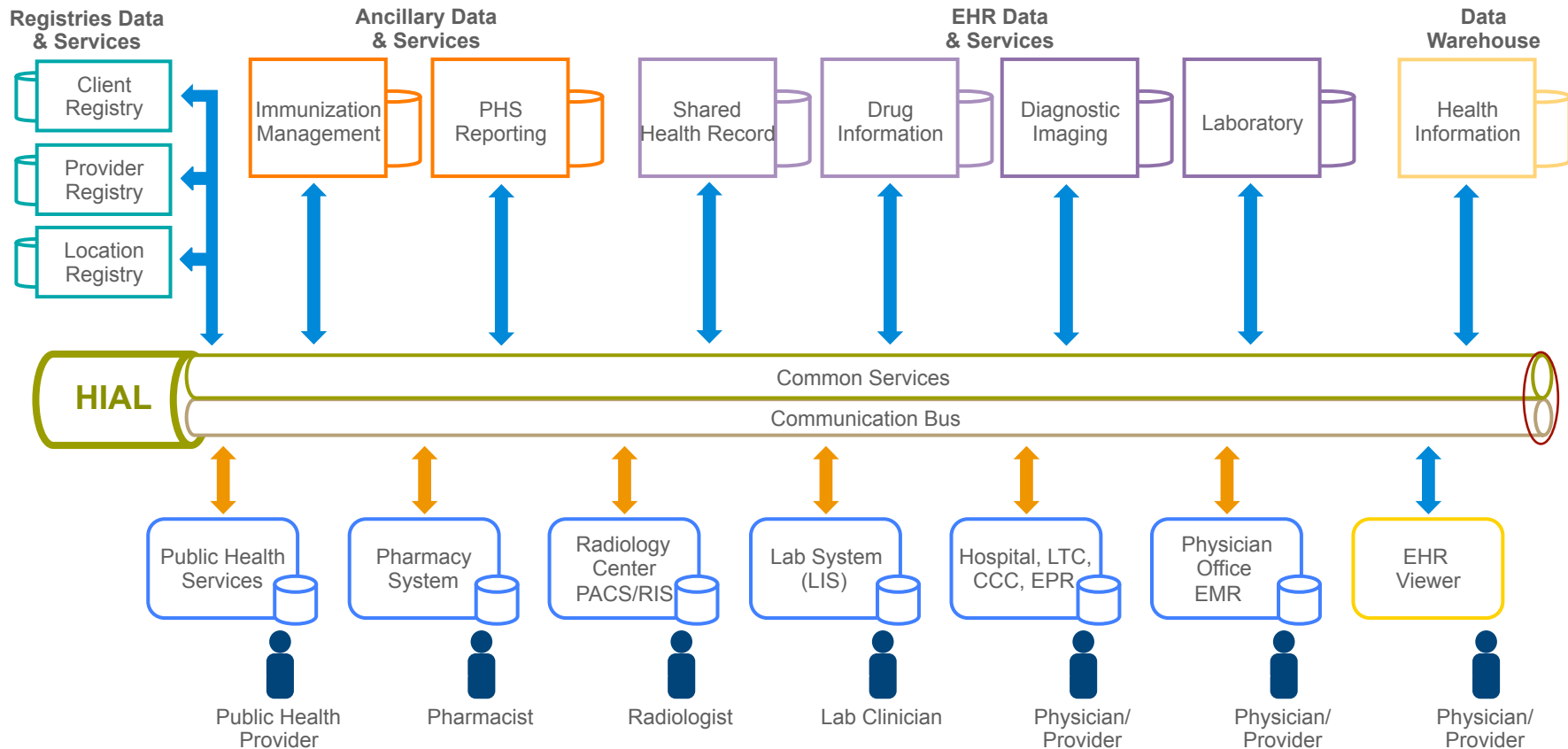
Demo of (my) Standards Spreadsheet

<http://hssp-security.wikispaces.com/file/view/EHRi+PS+Resources+and+Standards+20101016+draft-1.xls>

tab: new arch .
tab: standards

Infoway Blueprint EHRs Architecture

PROVINCIAL INFOSTRUCTURE

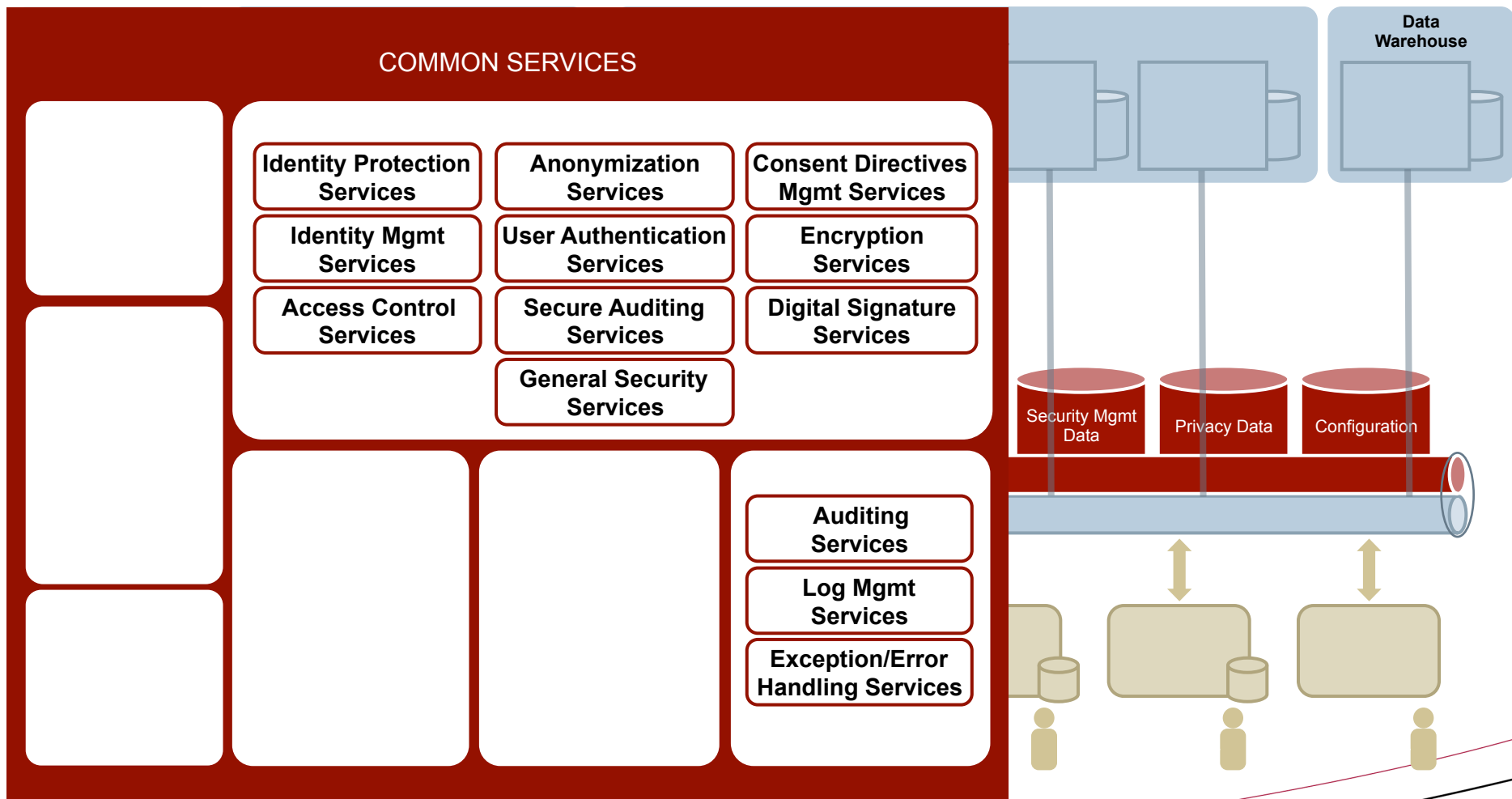


POINTS OF SERVICE

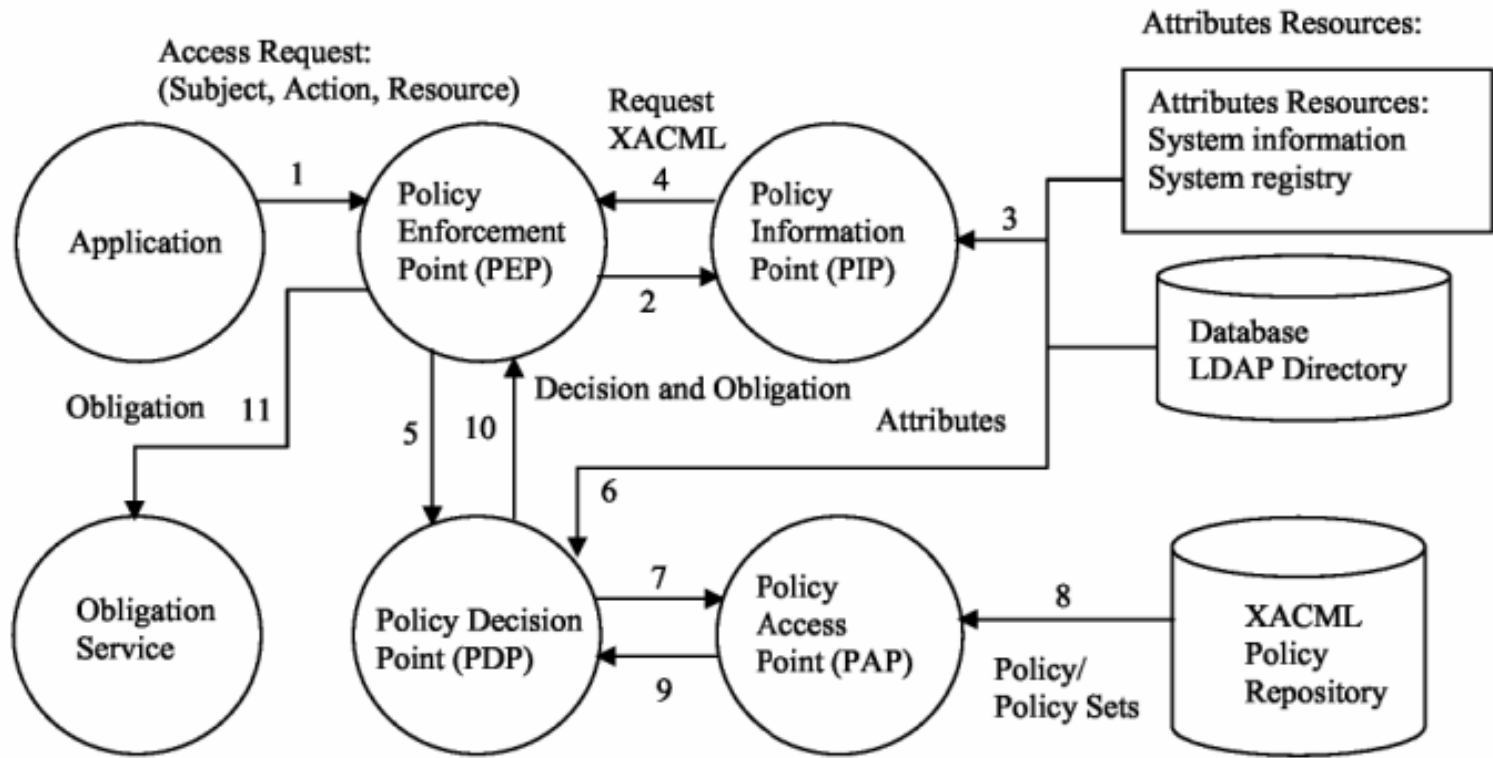
André M. Carrington

68

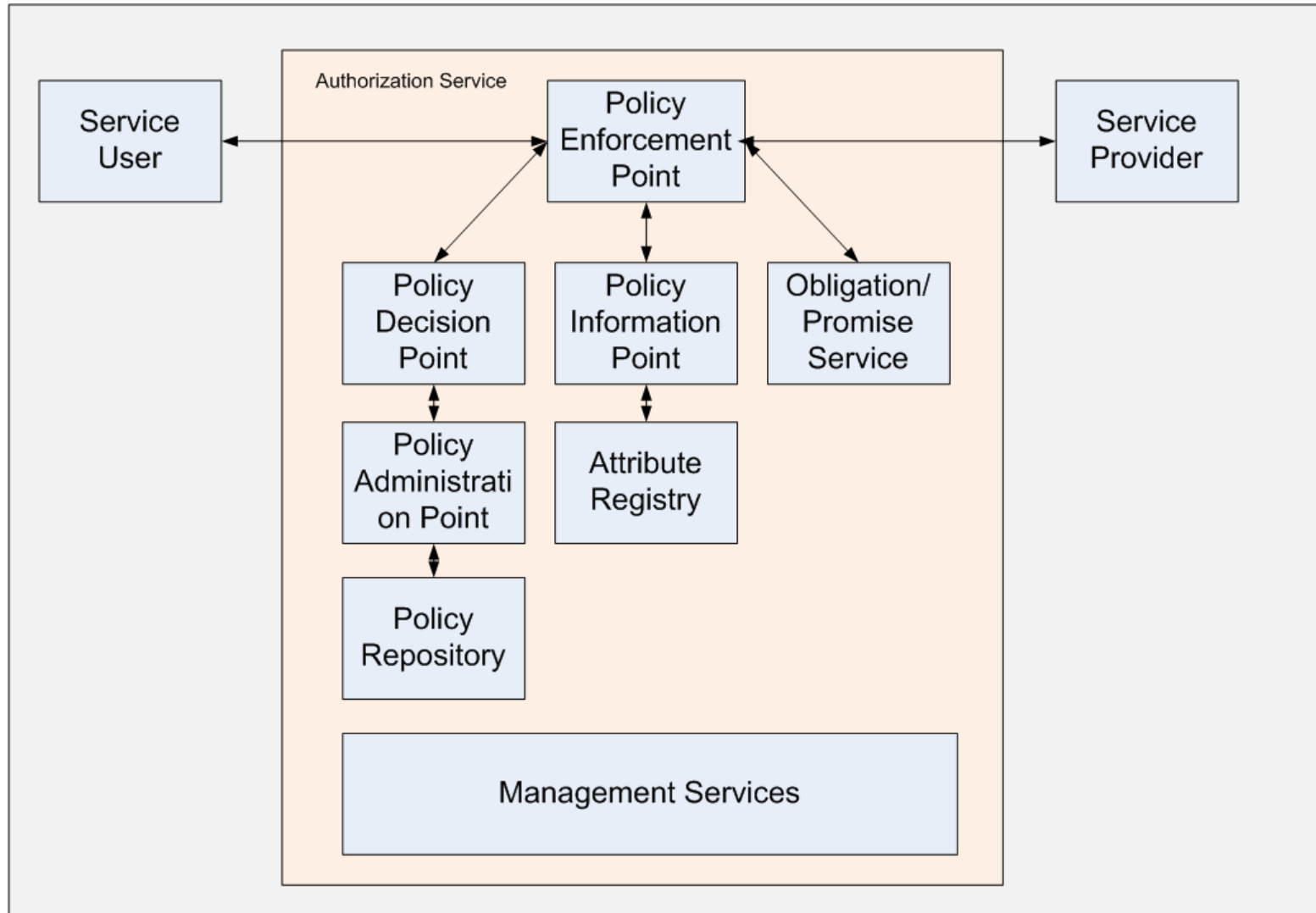
Infoway Blueprint Privacy & Security Conceptual Architecture



NIST / OASIS Access Control Model

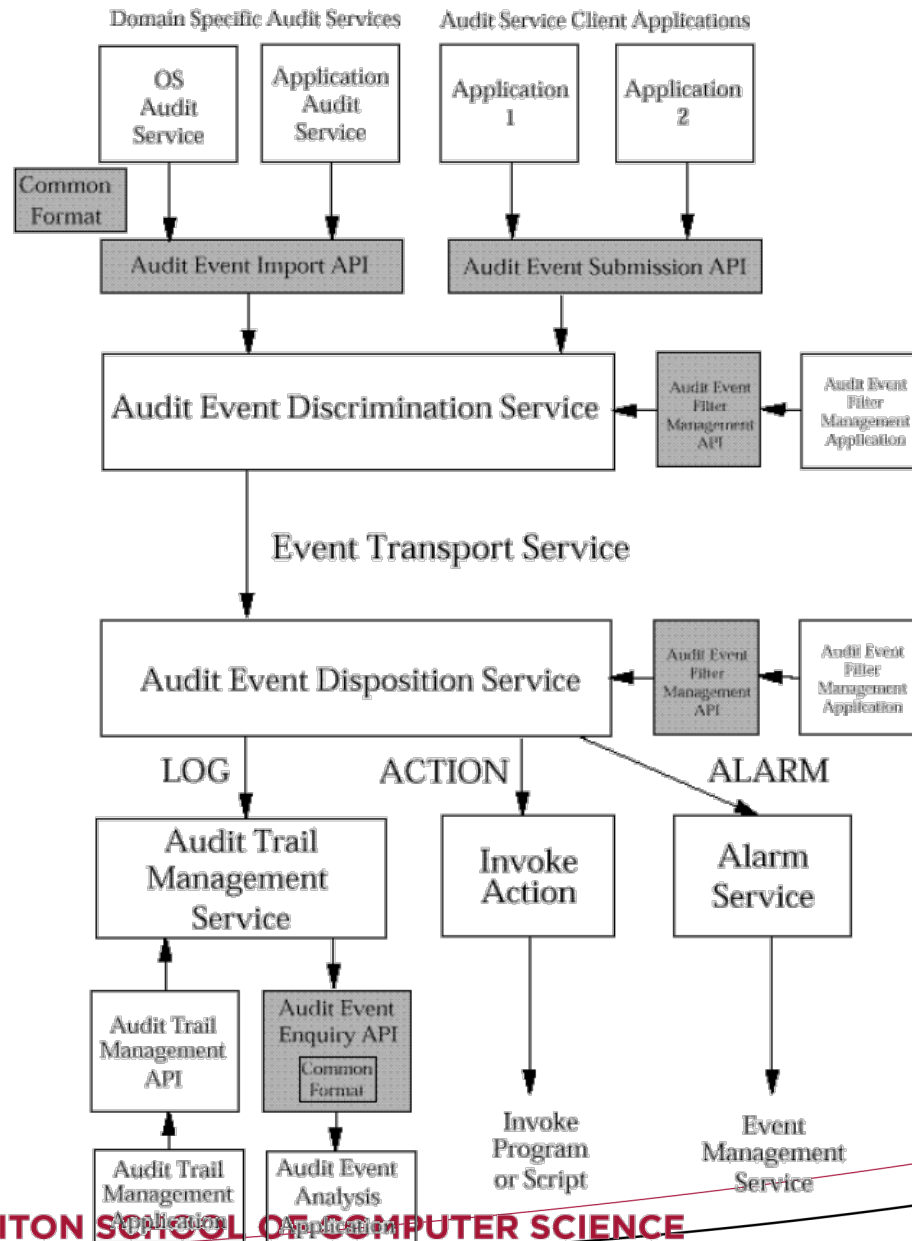


HL7 PASS Harmonized AC Model



André M. Carrington

The Open Group Distributed Audit Service



André M. Carrington

Common security design principles

- Need-to-know; least privilege
- Weakest link
- Separation of duties; isolation
- Keep it simple
- Defense in depth
- Fail safe
- Obscurity in IT is often a weak control
- Built-in not bolted on
- Specialization

Other Mantras

- **Prevent, Detect, Respond (PDR)**
- **Authentication, Authorization, Accounting (AAA)**
- **People, Process, Technology**

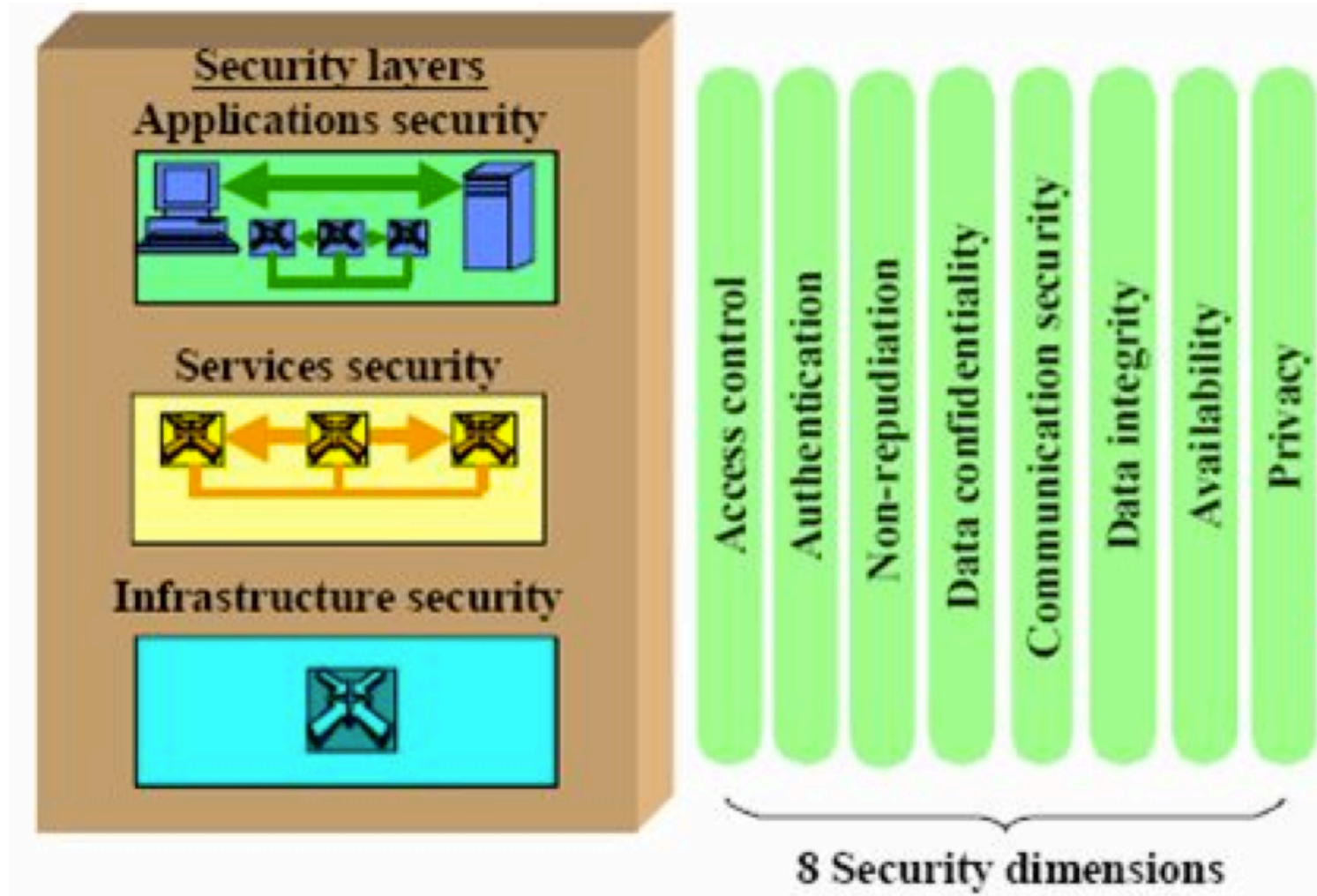
IBM Security Architecture based on ISO 7498-2

- Identification & Authentication
- Access Control
- Confidentiality
- Data Integrity
- Non-repudiation

- System Integrity

- Services Management
- Object Management
- Policy Management

ITU-T X.805 security framework



Privacy Principle, Policy or Concept Frameworks

- PIPEDA & the CSA Model Code
- Industry Canada PIPEDA Awareness Raising Tools (PARTS)
- ACIET's Pan-Canadian Health Information Privacy & Confidentiality Framework (model law for provinces)
- COACH 2009 Guidelines for the Protection of PHI
- HIPAA, EU (DP) Directive 95/46/EC
- AICPA / CICA / IIA Generally Accepted Privacy Principles
- Solove's privacy framework
- ISO 29100 privacy framework
- Adams' privacy framework

Privacy Architecture Frameworks

- CHI EHRS Blueprint Conceptual Privacy & Security Architecture
 - and the Blueprint P&S Requirements; P&S Use Cases
- COACH 2009 Guidelines for the Protection of PHI
 - and the 2010 Special Edition (for clinicians)
- Common Criteria
- ISO 29101 Privacy Reference Architecture
- Markle Foundation's Connecting for Health: Common Framework for Networked PHI

Security architecture frameworks

- ISO 27002 (formerly ISO 17799; BS 7799)
 - ISO 27001 (ISMS, discrete list of controls)
 - ISO 27799 (health)
- ISO 10181 series (or ITU-T X.810-816)
- ISO 13335 series (GMITS)
- ISO 7498-2
- ITU-T X.805 and ITU-T E.408
- OWASP

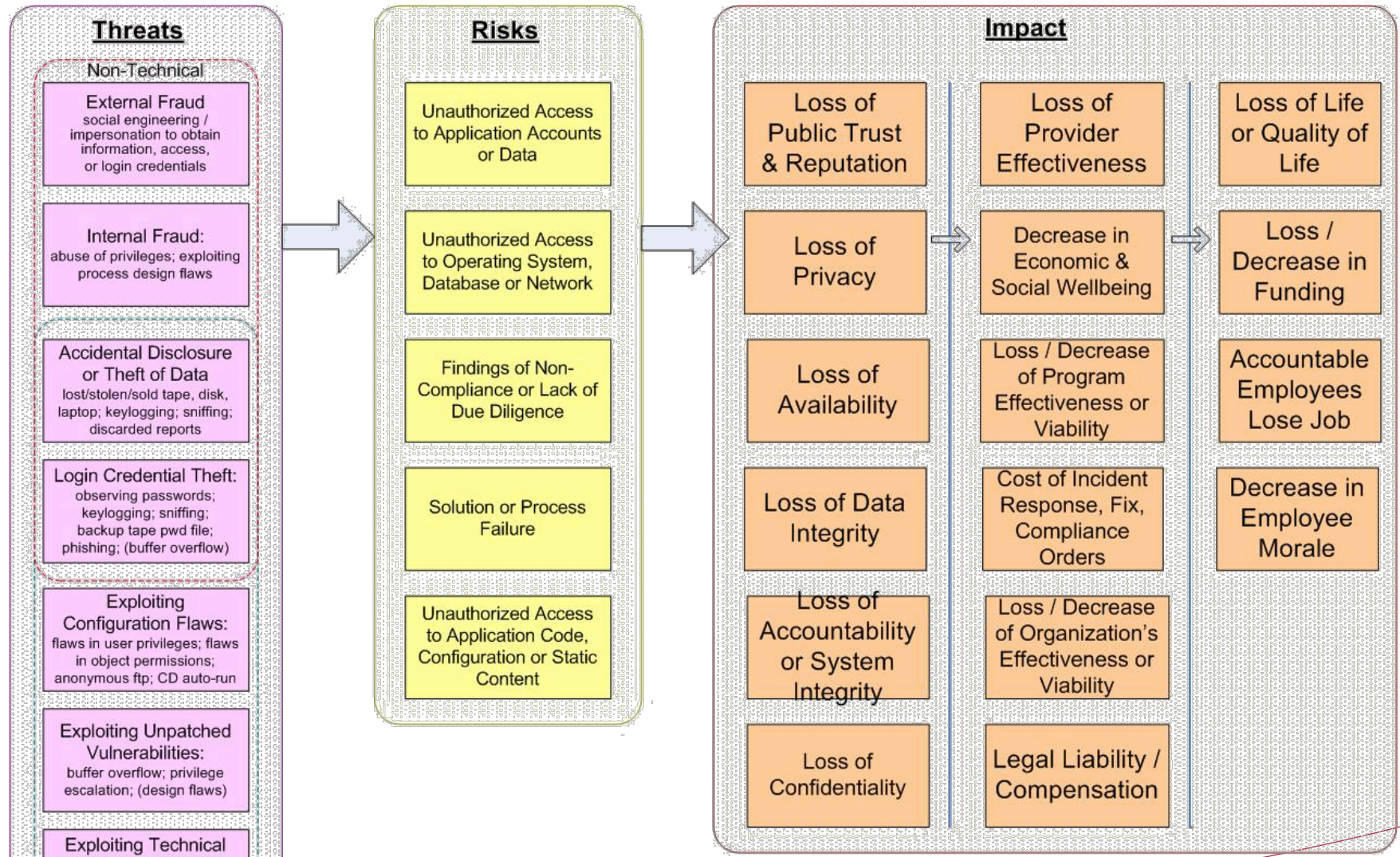
What ISO 27002 does not provide

- Clear linkages to SDLC & PMO processes
- Architecture!
 - Design principles
 - Design patterns
 - UML diagrams
- Requirements from abuse cases (e.g. OWASP)

My threat-risk model in HL7 & IHE security guides

http://gforge.hl7.org/gf/download/docmanfileversion/5519/7013/StdS_20100107_SW_7.4_HL7_Security_Cookbook_v2.41_DRAFT.docx

http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Whitepaper_Security_Cookbook_2008-11-10.pdf

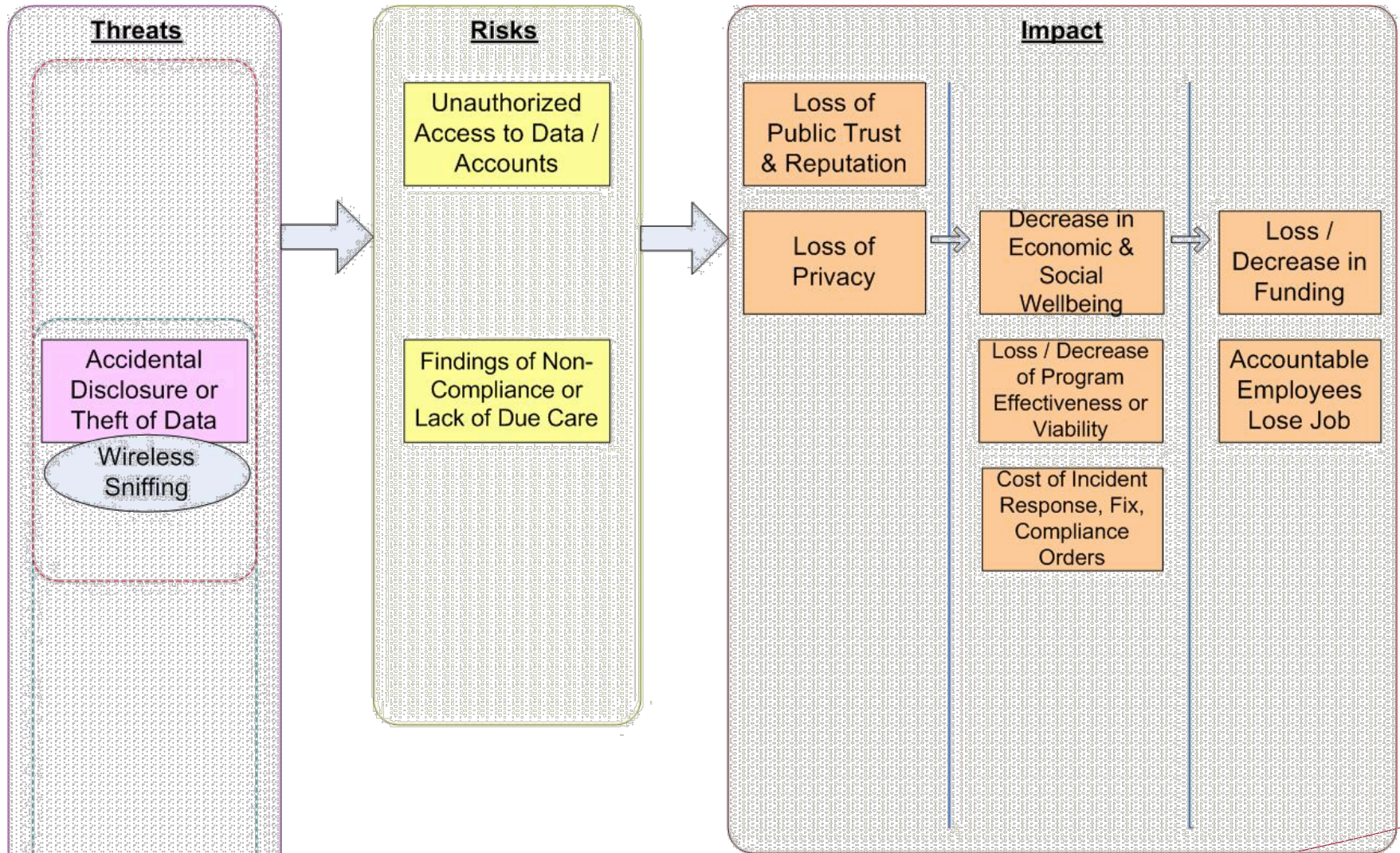


André M. Carrington

CHERITON SCHOOL OF COMPUTER SCIENCE

Source: Model and diagram based on prior work, copyrighted by Bedrock Security Services Inc., André Carrington

A walk through

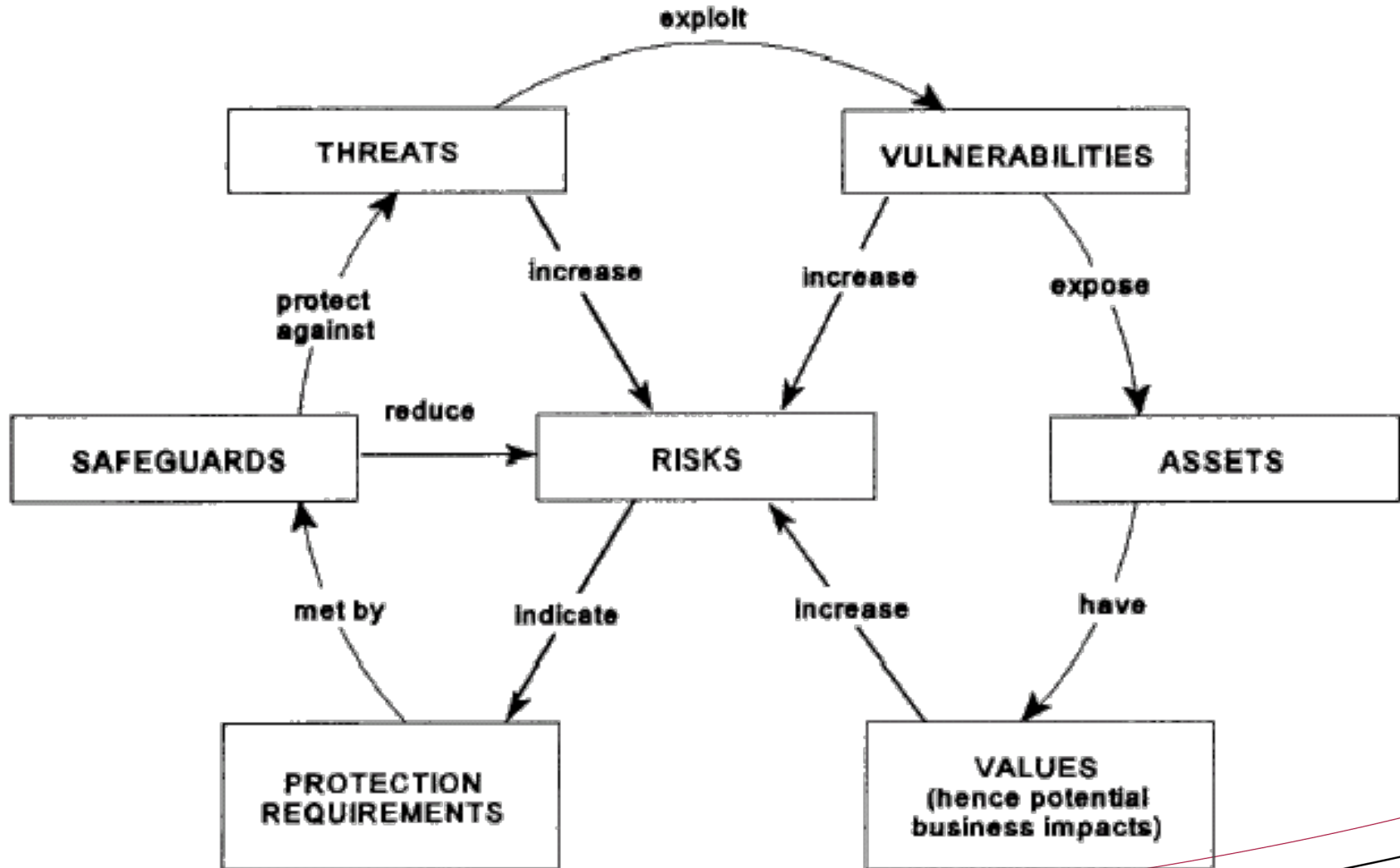


André M. Carrington

Boulanger's System Penetration Protocol

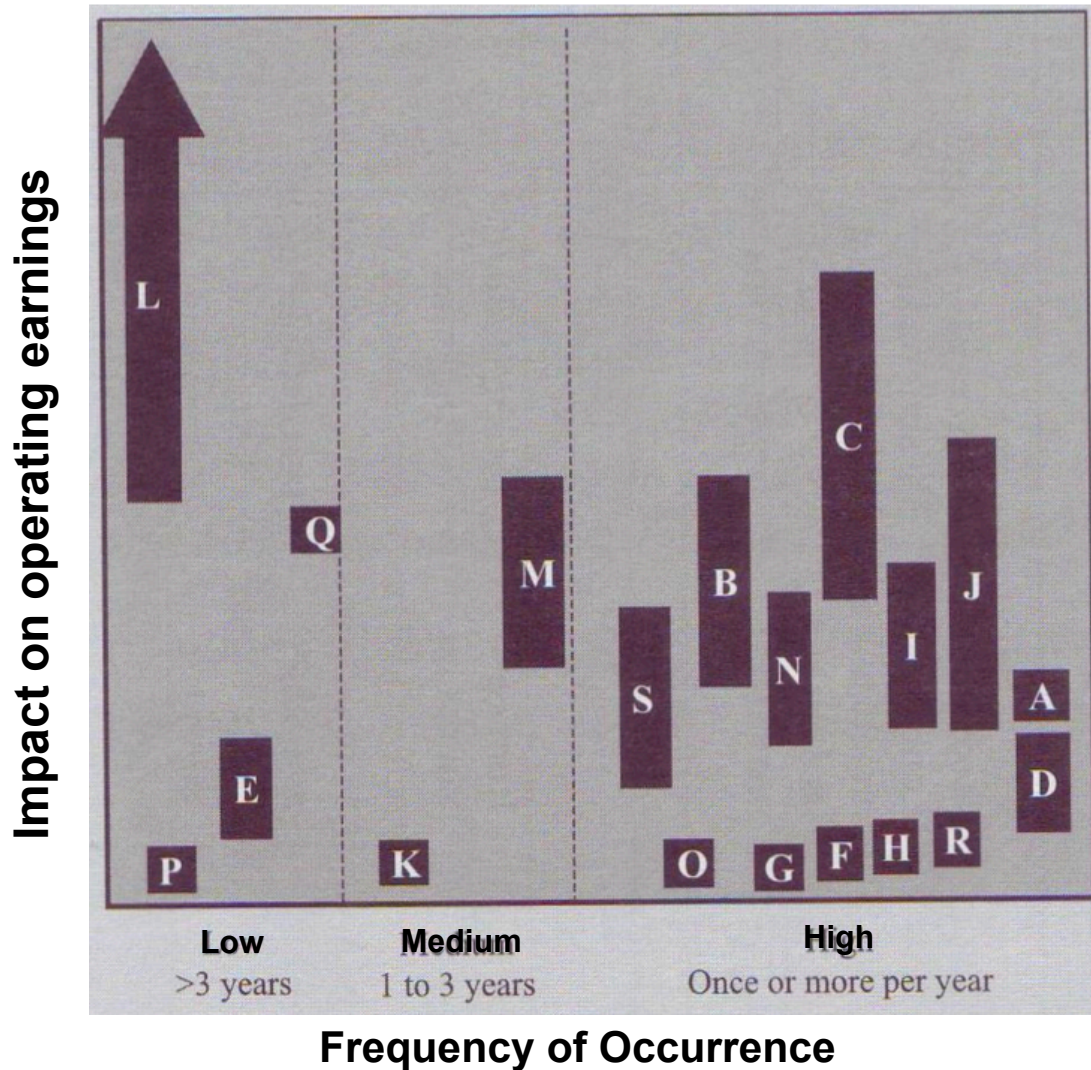
1. Reconnaissance: gather info about the target system or network
2. Probe & attack: probe the system for weaknesses and deploy tools
3. Toehold: exploit security weakness and gain entry into the system
4. Advancement: advance from an unprivileged to a privileged account
5. Stealth: hide tracks; install a backdoor
6. Listening post: establish a listening post
7. Takeover: expand control from a single host to other hosts

A general threat-risk model from ISO 13335



André M. Carrington

Risk Universe



- A – Access to capital
- B – Supplier Effectiveness
- C – Process Efficiency
- D – Process Effectiveness
- E – Litigation
- F – Asset Management
- G – Demand
- H – Intellectual Property
- I – Leadership
- J – Governance
- K – Systems
- L – Concentration
- M – Competition
- N – Interdependencies
- O – Economic
- P – Employee Safety
- Q – Government regulations
- R – Employee capabilities
- S – Data confidentiality

HL7 has an approach to architecture called SAIF that looks common

	Enterprise why - policy	Information what - content	Computational how - behaviour	Engineering where - implementation	Technical where - deployments
Conceptual	5 viewpoints				
Logical					
Implementable					

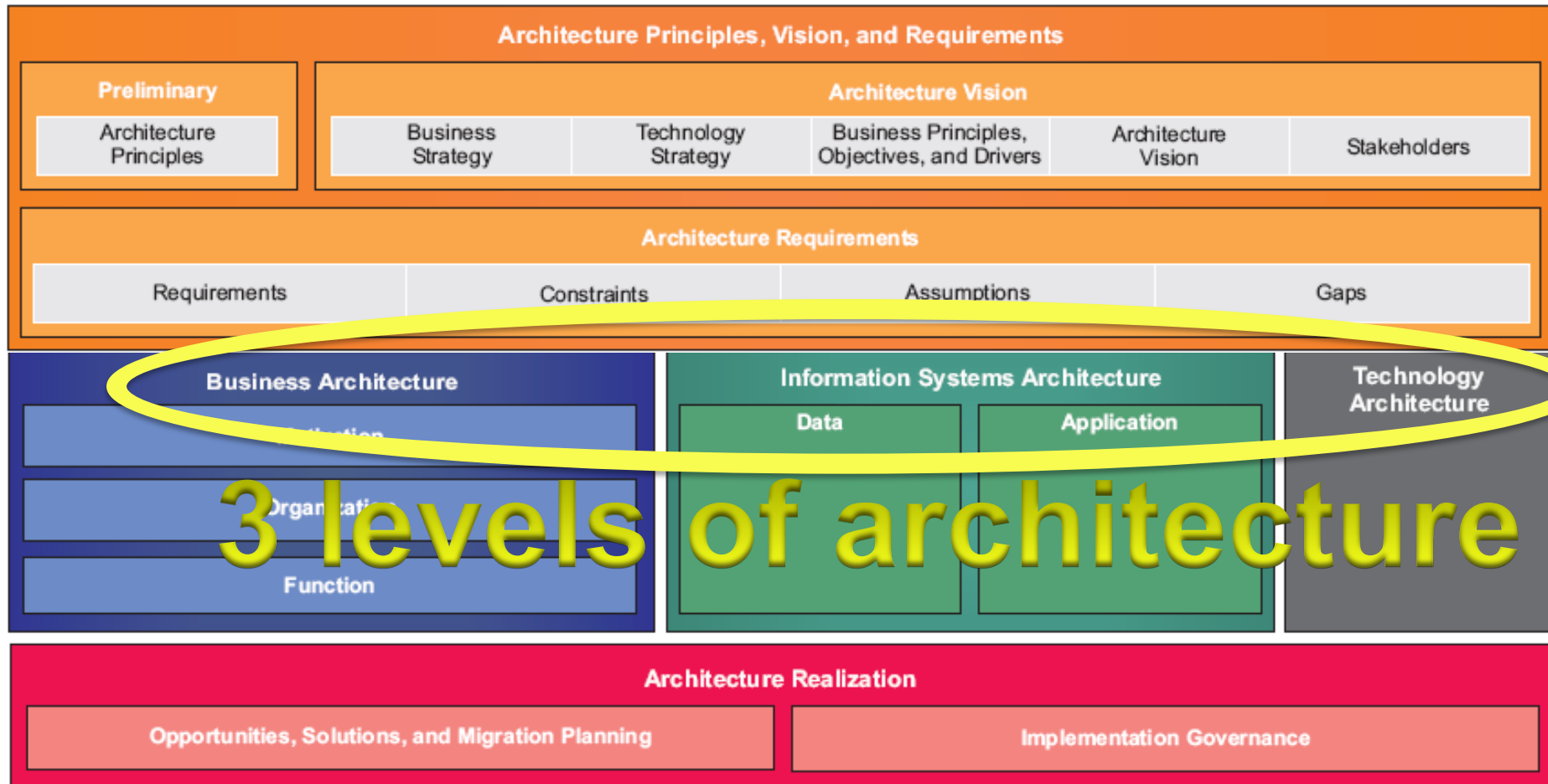
3 levels

It is similar to Zachman's framework

	What (Data)	How (Function)	Where (Locations)	Who (People)	When (Time)	Why (Motivation)
Contextual	List of things important to the business	List of processes that the business performs	List of locations in which the business operates	List of organizations important to the business	List of events/cycles important to the business	List of business goals/strategies
Conceptual	e.g. Semantic Model	e.g. Business Process Model	e.g. Business Logistics System	e.g. Workflow Model	e.g. Master Schedule	e.g. Business Plan
Logical	e.g. Logical Data Model	e.g. Application Architecture	e.g. Distributed System Architecture	e.g. Human Interface Architecture	e.g. Process Structure	e.g. Business Rule Model
Physical	e.g. Physical Data Model	e.g. System Design	e.g. Technology Architecture	e.g. Presentation Architecture	e.g. Control Structure	e.g. Rule Design
As Implemented	e.g. Data Definition	e.g. Program	e.g. Network Architecture	e.g. Security Architecture	e.g. Timing Definition	e.g. Rule Definition
	e.g. Data	e.g. Function	e.g. Network	e.g. Organization	e.g. Schedule	e.g. Strategy

André M. Carrington

TOGAF Content Framework



There are many proprietary methods

methods I've used, with formal training

IBM Enterprise Solution Structure
IBM Global Services Method
IBM OOAD Methodology
IBM Security Consulting Methodology
IBM Method for Architecting Secure Solutions
IBM PKI Consulting Methodology
Telus/Accenture Methods (UML)

methods I helped develop:

IBM Method for Architecting Secure Solutions

methods I learned but didn't apply:

SANS Ethical Hacking

André M. Carrington

methods I've worked with (no formal training)

IBM WSDDM Object Technology Method
ISO/IEC 12207 Software Dev Method
IBM Ethical Hacking
Zachman framework
IBM Enterprise Architecture Method
IPC Privacy Diagnostic Tool
RCMP TRA, RCMP/CSE Harmonized TRA
SANS Incident Response
COBIT, COBIT Online, COSO ERM
FMEA TRA
Capability Maturity Models
The Open Group Architecture Framework (TOGAF)

methods I've been exposed to at work:

TBS PIA, MGS (MBS) PIA
SAP Method
Deloitte Risk Assessments
SABSA (Sec Arch)
HL7 SAIF

Demo, again, of the Standards Spreadsheet

<http://hssp-security.wikispaces.com/file/view/EHRi+PS+Resources+and+Standards+20101016+draft-1.xls>

tab: methods

Agenda

privacy & security

- concepts
- architecture
- detailed design

ethics

trends (if time permits)

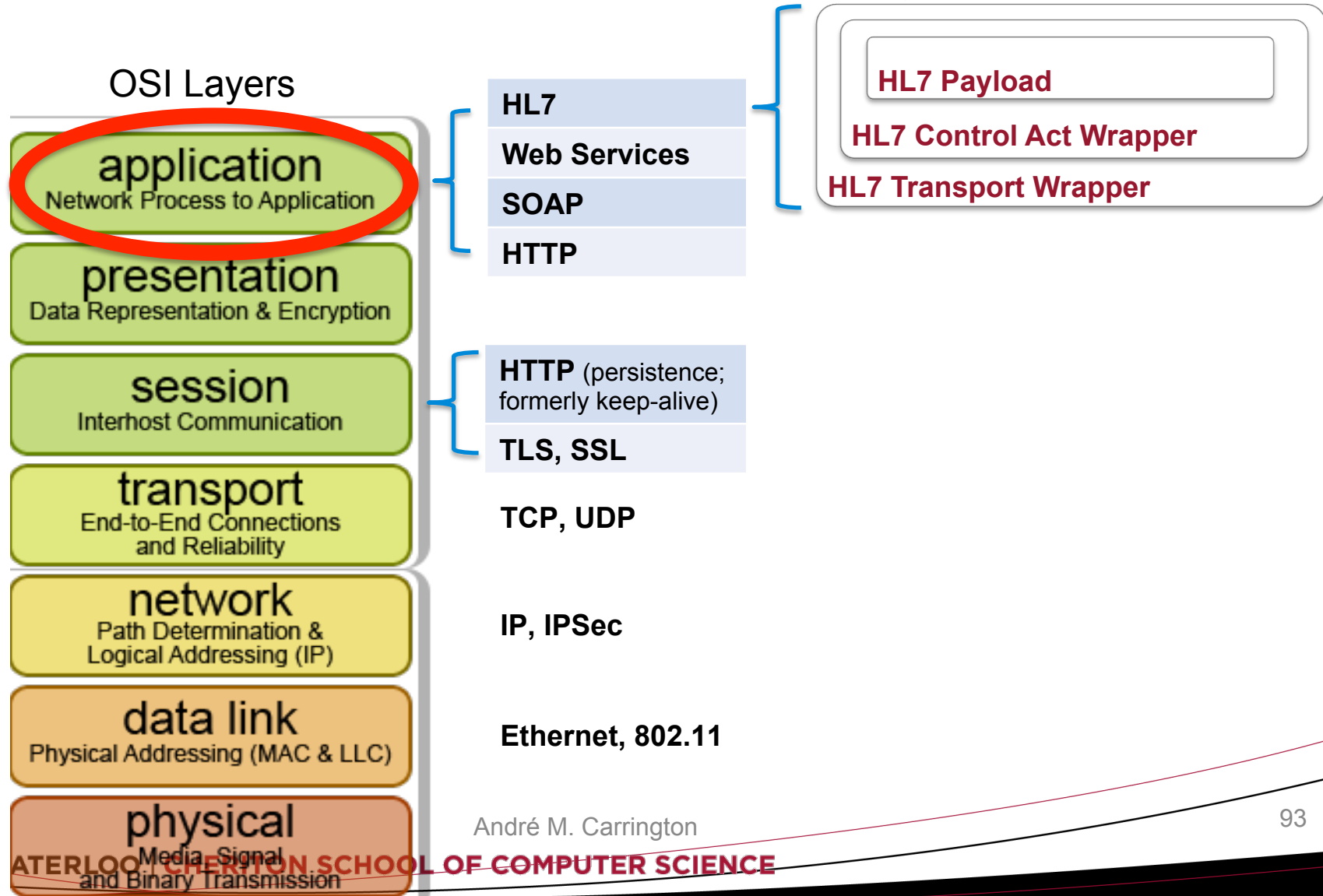
NHIN Connect & Secure E-mail

(USA)

[http://www.youtube.com/watch?
v=QSfeoV2EPR8](http://www.youtube.com/watch?v=QSfeoV2EPR8)
26:45 – 32:00

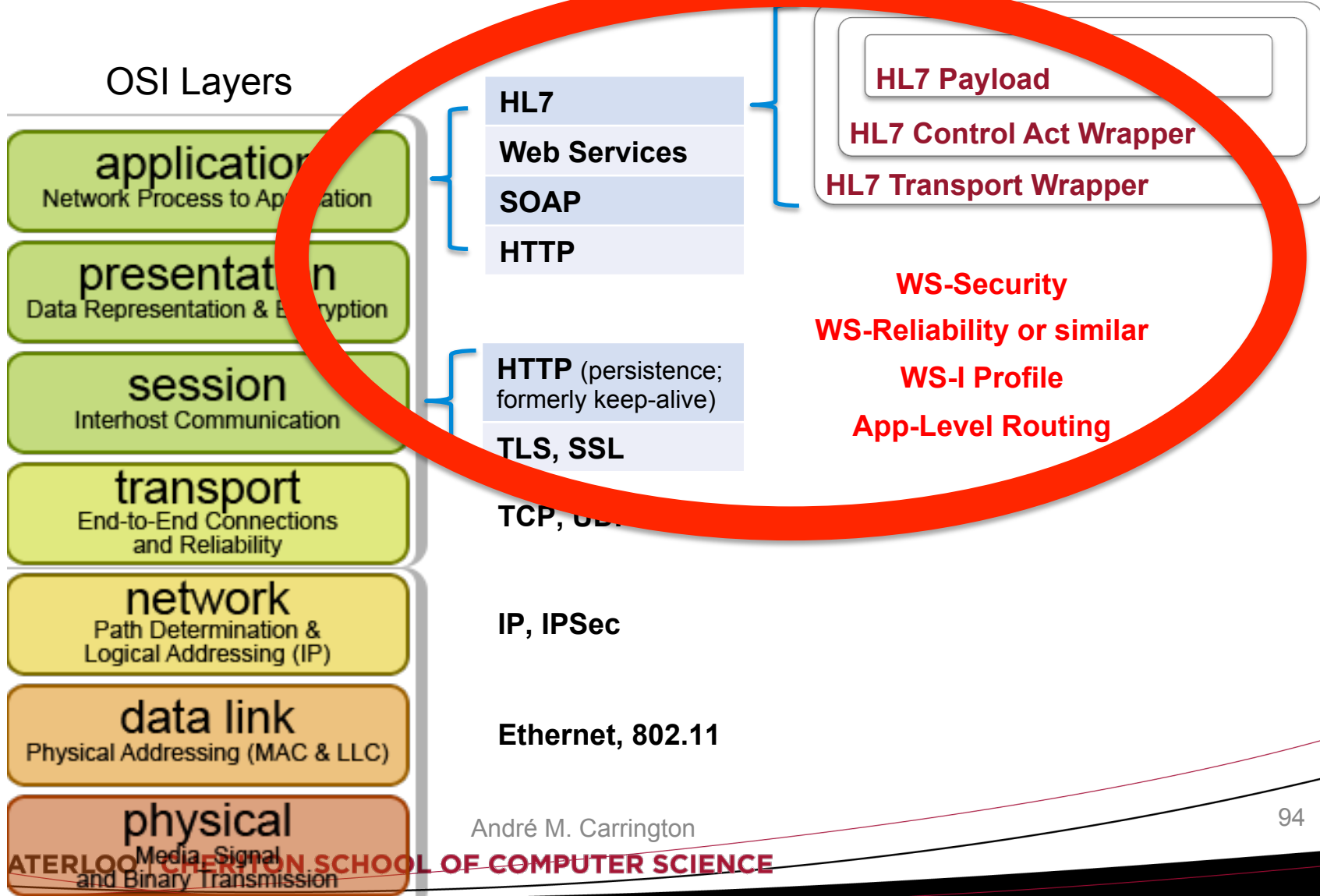
- fax paradigm
- EHR use case (similar to Canada)
- patient lookup misuse
- stalker problem
- problems patching certified software

Health Level 7 is a protocol at the 7th OSI layer.



André M. Carrington

Infoway's Transport Layer Interoperability spec uses...



André M. Carrington

Updates to cryptography in the TLI spec

1. authentication (dig sig) & key exchange
 - **RSA***, **DSS/DSA***, **ECDH****, **ECDHE****, **ECDSA****
 - ≥ 2048 bit RSA/DSS/DSA support required
 - ≥ 224 bit ECC required if supported, ECC preferred
 - for key exchange, ECDH not recommended, ECDHE ok
2. transport encryption
 - **AES*** (**recommended over**) **3DES/TDEA**
 - ≥ 128 bits (effective strength) support required
3. transport integrity was not updated due to insufficient support for interoperability

*affected, **new

Insufficient support for better transport integrity

SHA-1[^] and ideally SHA256^{**}, SHA384^{**}, SHA512^{**} to support hashes ≥ 256 bits, per SHS FIPS 180-3 (v3 Oct 2008)

Not supported in:

- TLS 1.0 (widely implemented)
- TLS 1.1 (not widely supported)
- AES Ciphersuites for TLS
- ECC: Suite B Profile for TLS (TLS 1.1 transitional profile)

Only supported in:

- TLS 1.2 (very sparsely supported)
- ECC: Suite B Profile for TLS (TLS 1.2 profile)
- ECC: TLS EC Ciphersuites w SHA-256/384 and AES GCM

*affected, **new, [^]CSEC/NIST deprecated end of 2010

Agenda

privacy & security

- concepts
- architecture
- detailed design

ethics

trends (if time permits)

Ethics: Primum Non Nocere

(do no harm)



Determinant Factors of Medical Practices

- What is the problem?
- What am I competent to do?
- What will produce the most desirable results?
- What will maintain or improve patient care?
- How strong are my beliefs in accuracy of my answers to questions above?

HI Applications: Appropriate Use

- First and foremost: human value
- Appropriate Use
 - Lab information system: *push for wider adoption*
 - Clinical expert systems: *apply extreme caution*
 - Error avoidance
 - Ethically optimized

HI Applications – Users and Educational Standards

- Right tool for right user is of high moral significance
- Diagnostic tool
 - For trained physician
 - User must be able to recognize error, and interpret the results appropriately
- Consumer-based HI product
 - General information/primer education material
 - Patient or caregivers as users, not trained
 - Patient specific consultation
 - Additional legal concerns related to negligence and product liability

Ethical Principles for Appropriate Use of CDS

- Use in clinical practices only after evaluation
 - Efficacy, cost, time
 - Perform the intended tasks
- Use by licensed professionals
 - Users able to make clinical decisions based on their qualification
 - Information systems should only serve to augment
- User training
 - Users need to be trained adequately for using a information product

Obligations and Standards for HI Professionals

- Ethics, standards and scientific progress
 - Professional-patient trust
 - Accuracy and performance
 - Acceptance by users, consequence for social and professional interactions
 - Context of use

Ten Criteria for HI System Scrutiny

- Work as designed
- Used as anticipated
- Produce desired results
- Work better than the procedures it replaced
- Cost effective
- Users trained specifically
- Anticipated long term effect on interaction
- Long term implication on health delivery
- Long term impact on the organization
- To what extent do effects depend on practice setting

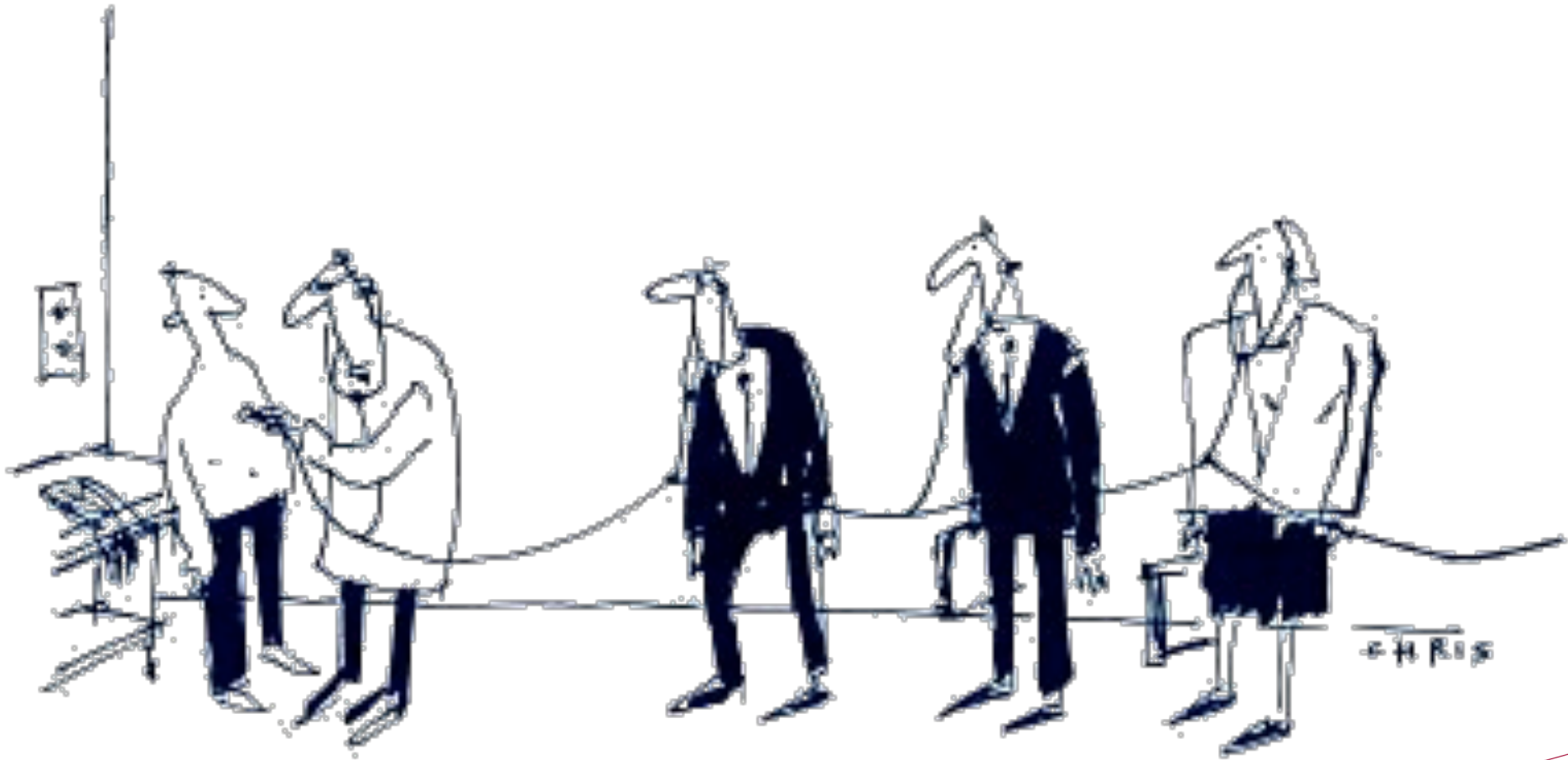
Issues of Ethical Importance in Consumer Health Informatics

- Peer review: who should be responsible to communicate accurate information to patient?
- Online consultation: professional qualifications, clinical judgment not based on face-face observation
- Support group: may provide false assurance and delay clinical actions

Social Challenges and Ethical Obligations

- Managed care based on statistical output of practice data
 - Danger of applying population based policy to an individual
 - Different goals may lead to different treatment choices, not just compliance to managed care “evidence”
- Danger of replacing human cognition for computer output
- and...

Ethics in Secondary Use



Purposes for Use (ISO DTS 14265)

- Increased demand for secondary use of patient information
 - Push for evidence-based medicine (as a recent trend)

Code	Classification Term
1	Clinical care provision to an individual subject of care
2	Emergency care provision to an individual subject of care
3	Support of care activities within the provider organisation for an individual subject of care
4	Enabling the payment of care provision to an individual subject of care
5	Health service management and quality assurance
6	Education

Code	Classification Term
7	Public Health Surveillance, Disease Control
8	Public safety emergency
9	Population health management
10	Research
11	Market Studies
12	Legal Procedure
13	Subject of Care Uses
14	Unspecified

AFN Resolution 32/2004

- THEREFORE BE IT RESOLVED that the AFN...remind the federal government that it has never sanctioned any government or agency to enter First Nations land for the purpose of data collection and that...it is the sovereign and sole right of each First Nation Government and citizen to determine their participation in any data collection process;

...

AFN Resolution 32/2004

- THEREFORE BE IT RESOLVED that the AFN...remind the federal government that it has never sanctioned any government or agency to enter First Nations land for the purpose of data collection and that...it is the sovereign and sole right of each First Nation Government and citizen to determine their participation in any data collection process;
- FURTHER BE IT RESOLVED that First Nations...not support the implementation of external data collection processes within First Nation territories if the First Nations established principles of Ownership, Control, Access and Possession (OCAP) regarding health data and health information are not respected;

...

Research Ethics Boards (REBs)

e.g. UW's CREC

- 1 Faculty rep from Optometry
- 1 Faculty rep from Pharmacy
- 1 Clinician (clinical trials research), or Pharmacologist or Immunologist/Toxicologist
- 2 Clinical Physicians (clinical trials research)
- 1 Lawyer (prefer clinical trials research)
- 1 Community Member (unaffiliated)
- Director, Office of Research Ethics (ex-officio)
- Anticipated 1 member will have expertise in stats

REB Wizard & Uniqueness

“The percentage of the population that is unique on the set of quasi-identifiers that are being considered” – El Emam

- commonly used in statistical disclosure control
- used for more than 20 years re census data in many countries including Canada and the US
- based on the population and thus pertains to any data set

<http://www.ehealthinformation.ca/rebwizard/ca/index.asp>

What we've covered

privacy & security

- concepts
- architecture
- detailed design

ethics

trends (if time permits)

Questions?

André M. Carrington
amcarrin@uwaterloo.ca

Inherent risks are evolving

↑ consumer access ↑ data sharing ↑ APT ↑ cloud computing	↑ threat
↑ information collection ↑ information aggregation	↑ asset value
↑ privacy awareness	↑ impact

↑ Information Collection

- Bytes of data collected re live births, health care cost data and grocery purchases...

Examples	1983	1996
Each birth	280	1864
Each hospital visit	0	663
Each grocery visit	32	1272

Figure 1 Estimated growth in data collections (per encounter) in Illinois (in bytes)

Source: Latanya Sweeney

André M. Carrington

Five fastest rising breach categories in Canada in 2009

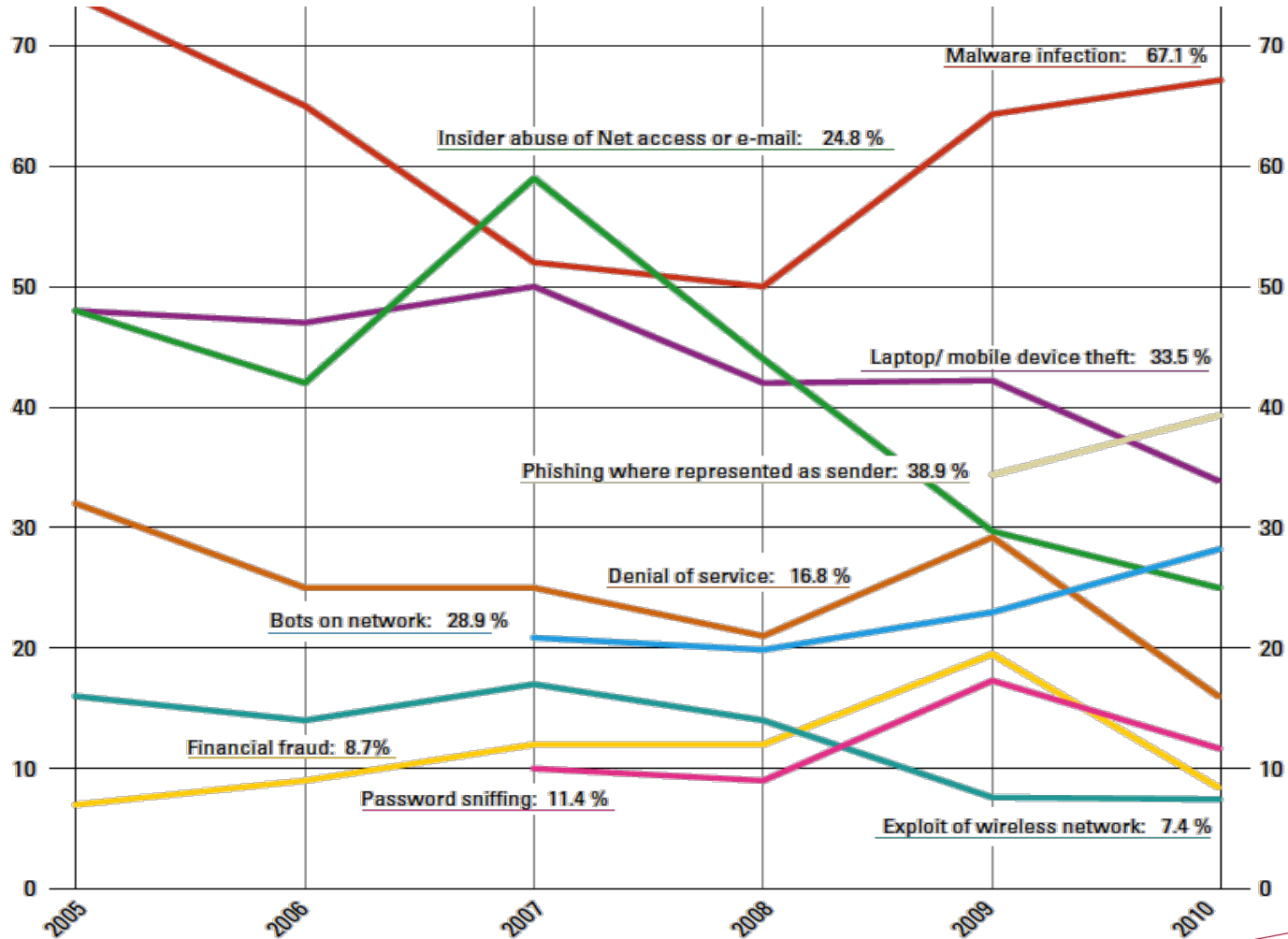
1. Unauthorized access to information by employees (up by 112%)
2. Bots within an organization (up by 88%)
3. Financial fraud (up by 88%)
4. Theft of proprietary information (up by 75%)
5. Laptop or mobile-device theft (up by 58%)

-- Telus/Rotman Infosec Survey

Changes in Infosec 2008 (UK)

- viruses are no longer the single greatest cost of incidents
- increase, 2% to 7%, IT Security budget expenditure
- increase, 5% to 14%, use of strong authentication
- increase, 5% to 11%, use of BS7799 / ISO27002
- companies that carry out risk assessment are four times as likely to detect identity theft as those that do not.

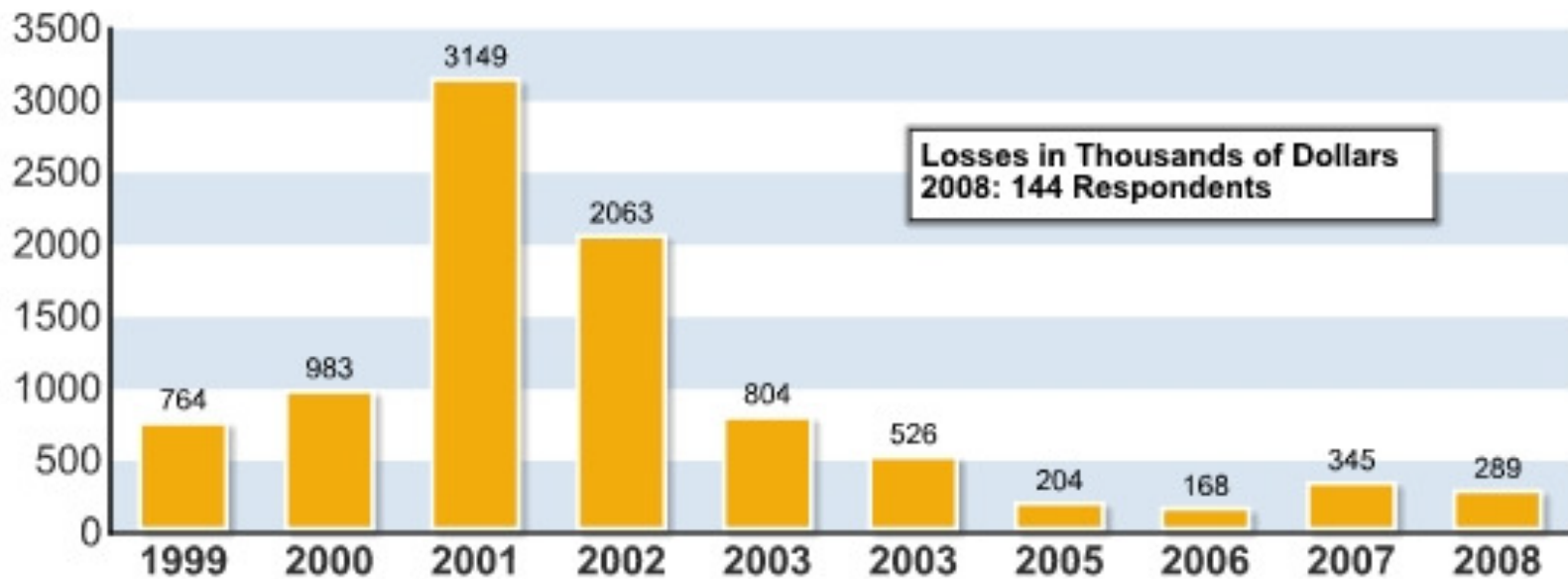
The threat & risk data we have...



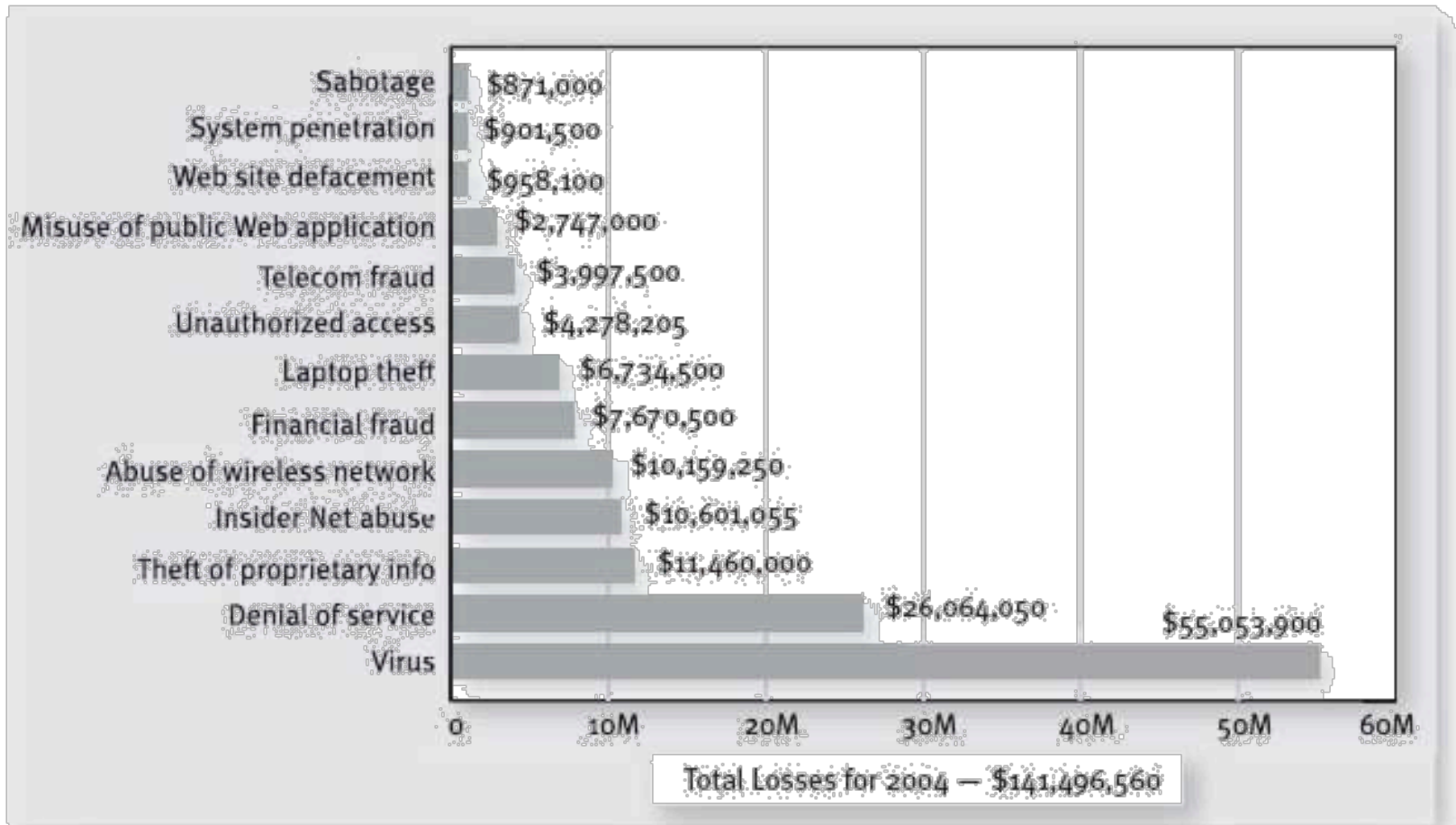
André M. Carrington

...is aggregate, sparse...

Figure 14: Average Losses Per Respondent



...and inconsistent over time...



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

2004: 269 Respondents

André M. Carrington

121

...but very informative nonetheless.

	Small (<50 staff)	Large (>250 staff)	Very Large (>500 staff)
Companies that had a security incident in the last year	45%	72%	96%
Average number of incidents, median (mean)	6 <i>(100)</i>	15 <i>(200)</i>	>400 <i>(>1,300)</i>
Average cost of worst incident in year	£10k to £20k	£90k to £170k	£1m to £2m

Is health care different from other industries?

- Flight-critical vs. mission critical
- A privacy breach regarding health information may be irreparable
- Doctors as independent end-users
 - their buy-in is essential
- Public funding/law vs. Private competition
 - incentives to integrate
- Lock-boxes (informational consent directives)

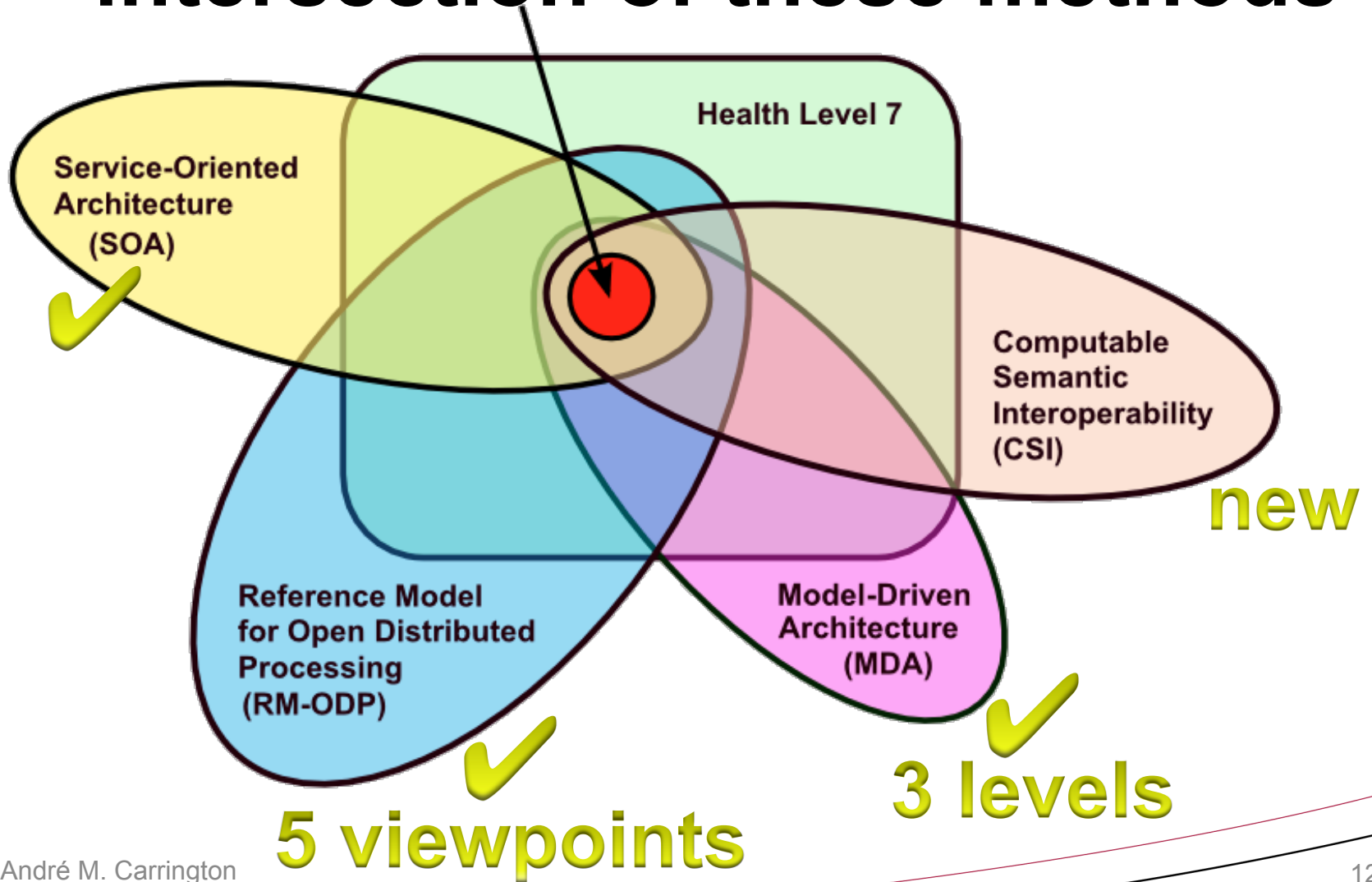
Elements of Threat Risk Assessment

- Assets
- Sensitivity
- Threat agents
- Vulnerabilities
- Controls
- Risk
- Residual Risk
- Recommendations

Elements of Privacy Impact Assessment

- Scope
- Legislative Authority
- Requirements Analysis
- Data Clusters, Actors, Data Flows, Collection / Use / Disclosure
- Privacy Principles Analysis
- Risk Assessment
- Recommendations

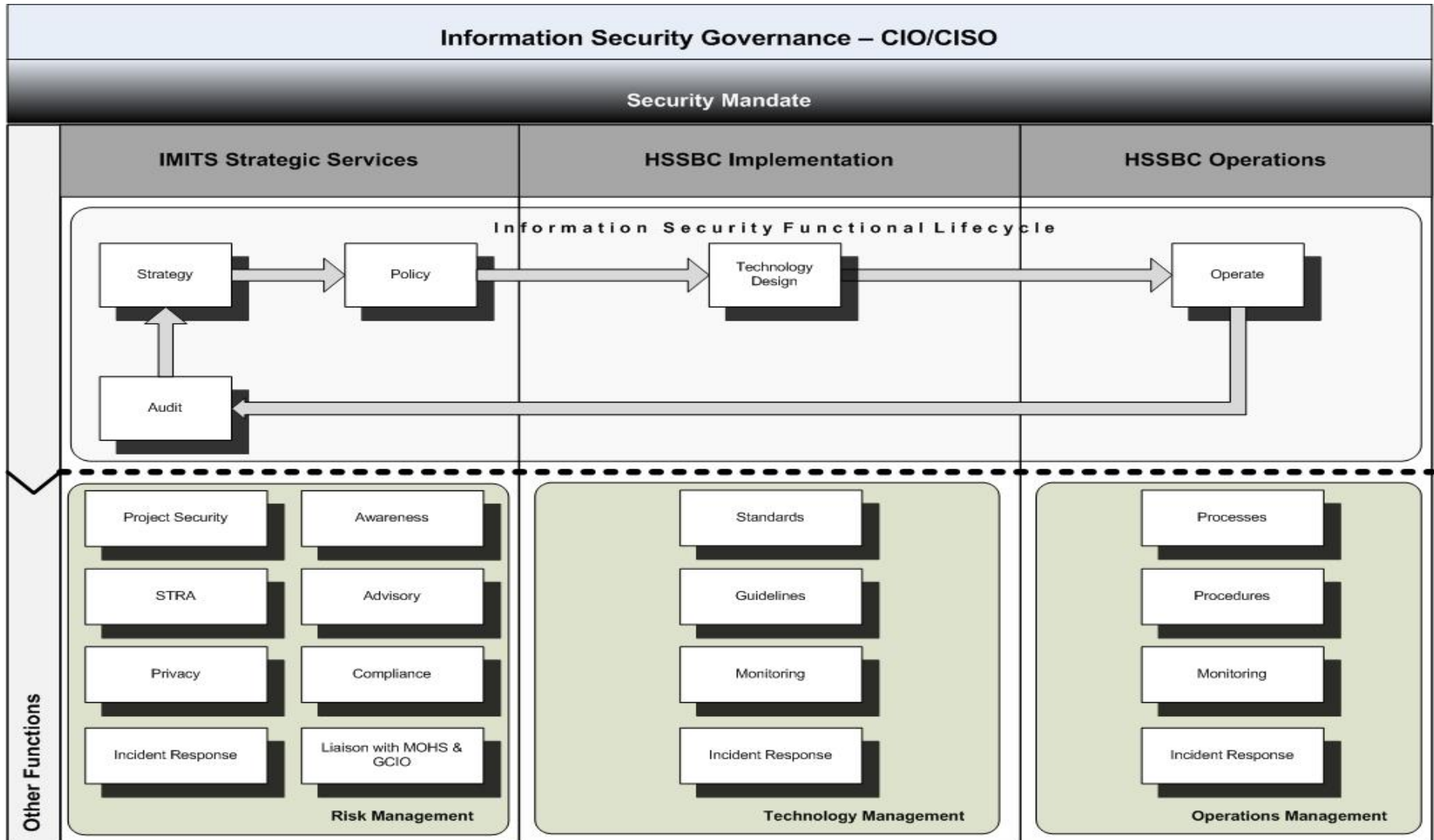
HL7 SAIF is at the intersection of these methods



Related topics not covered

- Access to Information
- Governance - IT, Data, in general
- Risk Management
- Business Continuity & Disaster Recovery
- Provenance
- Audit

BC Public Health Infosec Governance



André M. Carrington

IT Governance Institute Objectives

- **Strategic Alignment**
 - aligning with the business and collaborative solutions
- **Value Delivery**
 - optimising expenses and proving the value of IT
- **Risk Management**
 - safeguarding assets, disaster recovery and continuity of operations
- **Resource Management**
 - optimising knowledge and IT infrastructure
- **Performance Measurement**
 - performance measurement, tracking project delivery and monitoring IT services

IT Infrastructure Library (ITIL)

Service Support

- Incident management
- Problem management
- Config. management
- Change management
- Release management

Service Delivery

- Service level management
- Financial management for IT
- Capacity management
- IT service continuity mgmt
- Availability management

and lesser known volumes on:
Security Management, etc.

IBM Data Governance (Maturity) Model

- Organizational Awareness
- Policy
- Stewardship
- Value Creation
- Data Risk Management
- Security / Privacy / Compliance
- Data Architecture
- Data Quality
- Data Classification / Metadata
- Information Lifecycle Management
- Audit & Reporting