

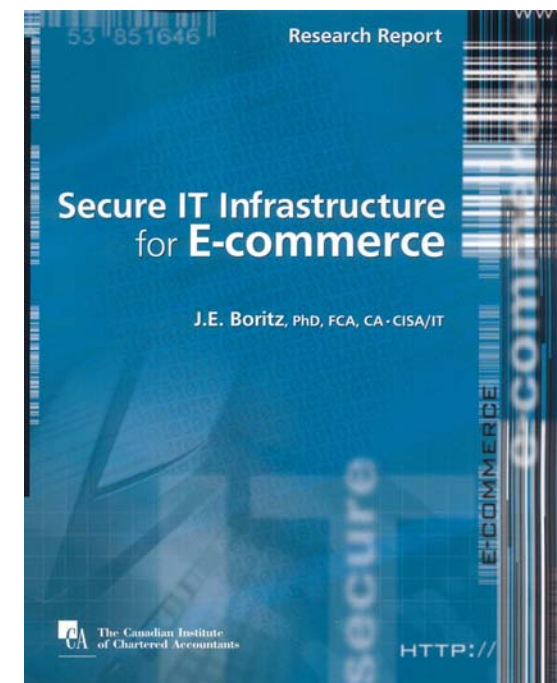
Secure IT Infrastructure for E-Commerce

J. Efrim Boritz

University of Waterloo

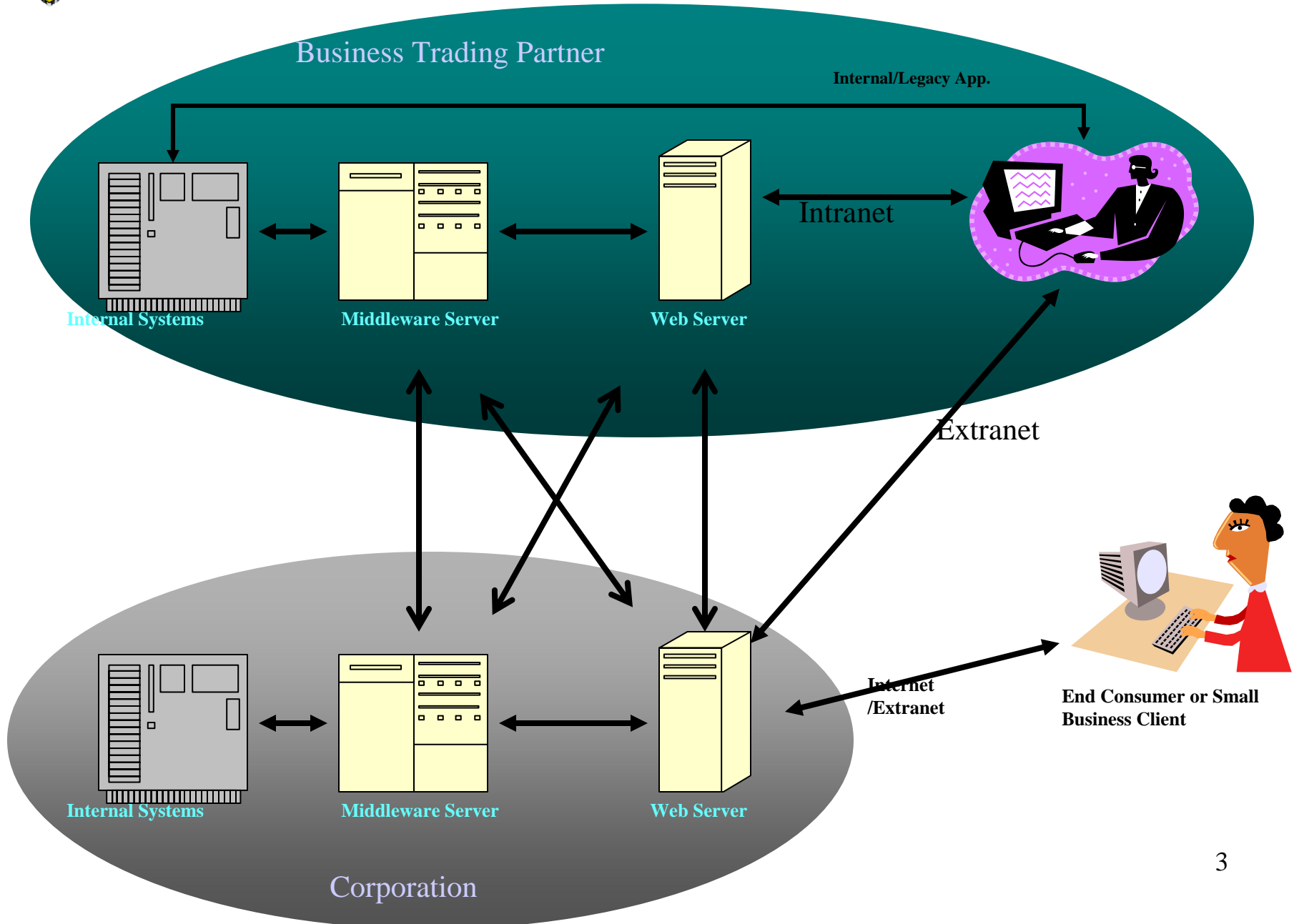
Centre for Information Systems Assurance

January 6, 2006



Acknowledgements

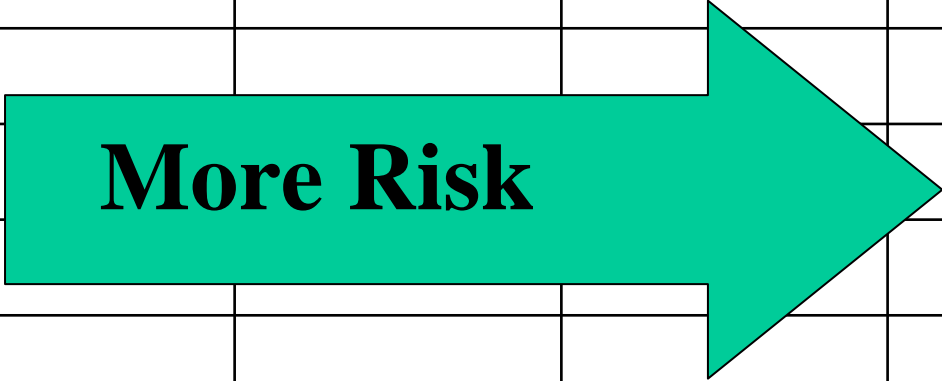
- Sponsors of the University of Waterloo Centre for Information Systems Assurance
 - Canadian Institute of Chartered Accountants
 - Toronto Chapter of ISACA and other Canadian Chapters
 - International HQ of ISACA
 - University of Waterloo
- Participants in focus group
- Research funding provided by CICA
- Research assistance by Malik Datardina, MAcc , CA•CISA





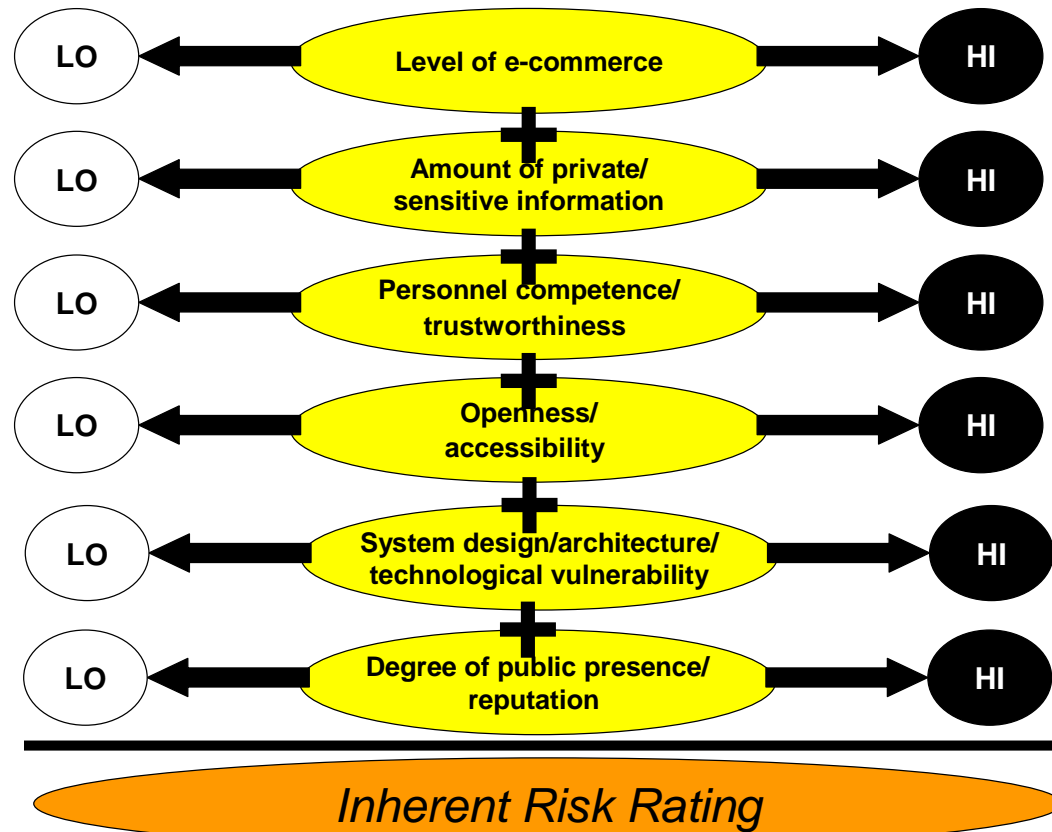
E-Commerce Risk Factors

	Point of presence	Inquiry and communication	Payment	Integration with back-office ^[1]
Trust/Risk Issues				
Availability				
Asset safeguarding				
Confidentiality/ Privacy				
Processing Integrity				
Authenticity of source				
Quality of goods/services				
Management Skill				

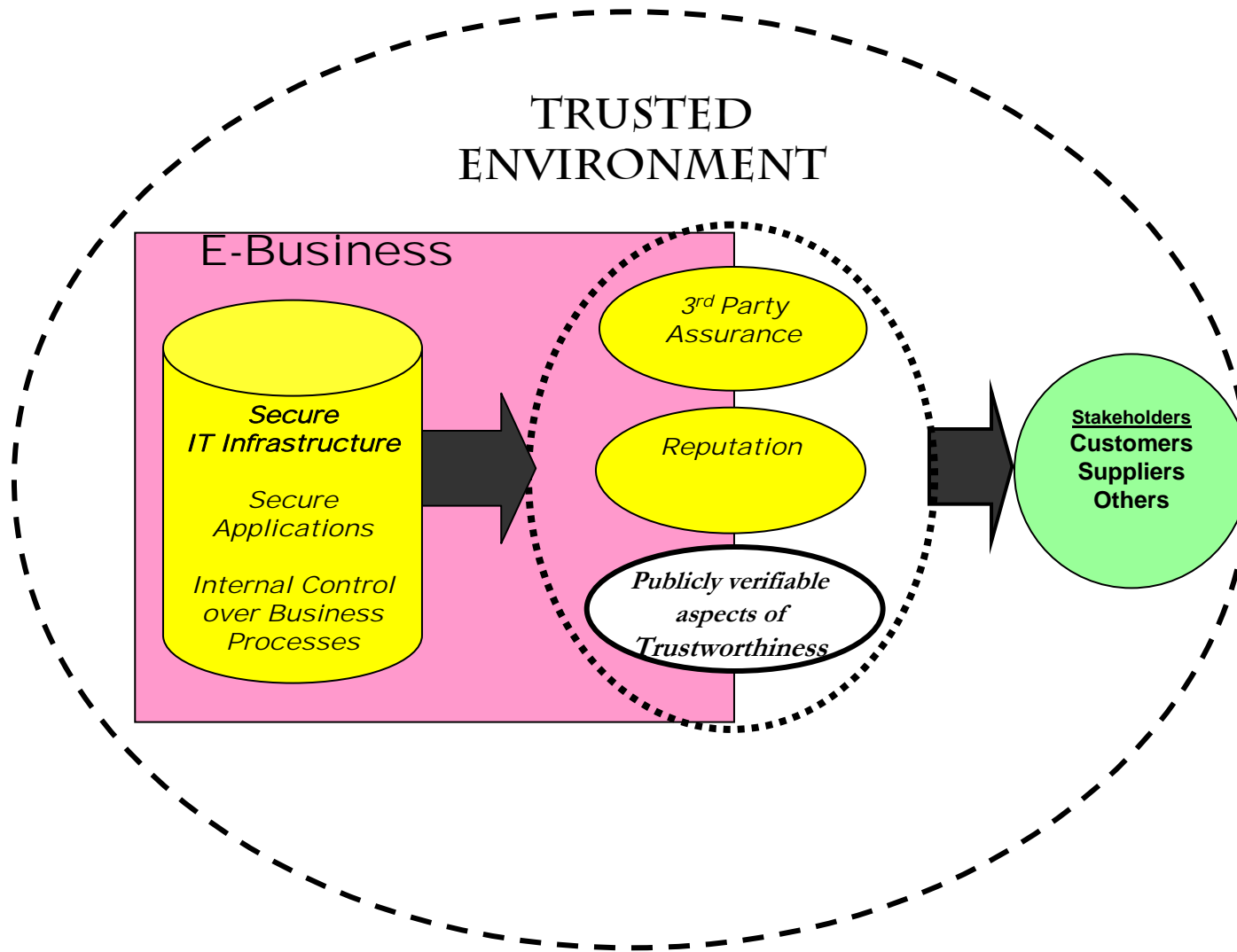


[1] Integration with back office includes inventory status checking during order processing, shipping information, scheduling installation, etc.,

E-Commerce Risk Factors



Security and Trust



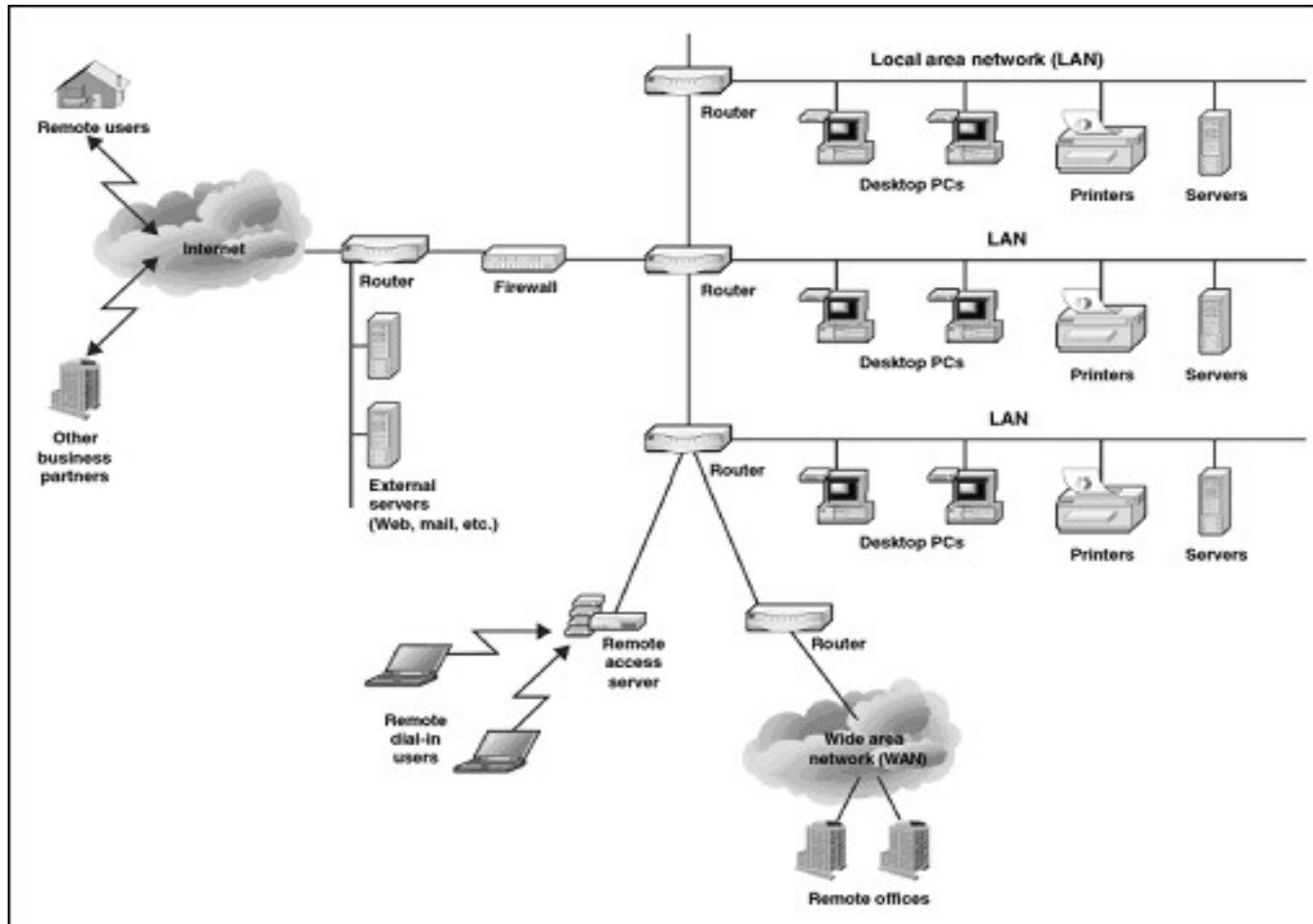
**Sources of Risk
in E-Commerce
Business Models**

Security Components

IT Infrastructure Components

A B C D E F G

- 1.**
- 2.**
- 3.**
- 4.**
- 5.**
- 6.**
- 7.**
- 8.**



Source GAO 04-467 March 2004

The IT Infrastructure... Is More Than Just Hardware and Software

Element/Literature Reference	Zachman; in Burgezz (1992)	Davenport and Lindner (1993)	Henderson and Venkatraman (1993)	Duncan (1995)	ITIL (1996)	Abcouwer and Truijens (1997)	Bharadwaj (2000)	Byrd and Turner (2000)	ISACA – COBIT (2000)	Koussik and Joodi (2000)	CICA – ITAC (2001)	Hagel and Brown (2001)	IBM (2001)	Hazra (2002)	Weill and Vitale (2002)
1.IT Architecture and Standards			√			√				√					
1.IT Components	√	√	√	√		√	√		√	√	√		√		√
1.Communications Infrastructure	√			√								√			
1.Shared and Standard Applications					√	√						√			√
1.Shared IT Services												√		√	√
1.IT Enabled Intangibles	√						√								
1.Human IT Infrastructure	√	√	√				√	√	√		√				√

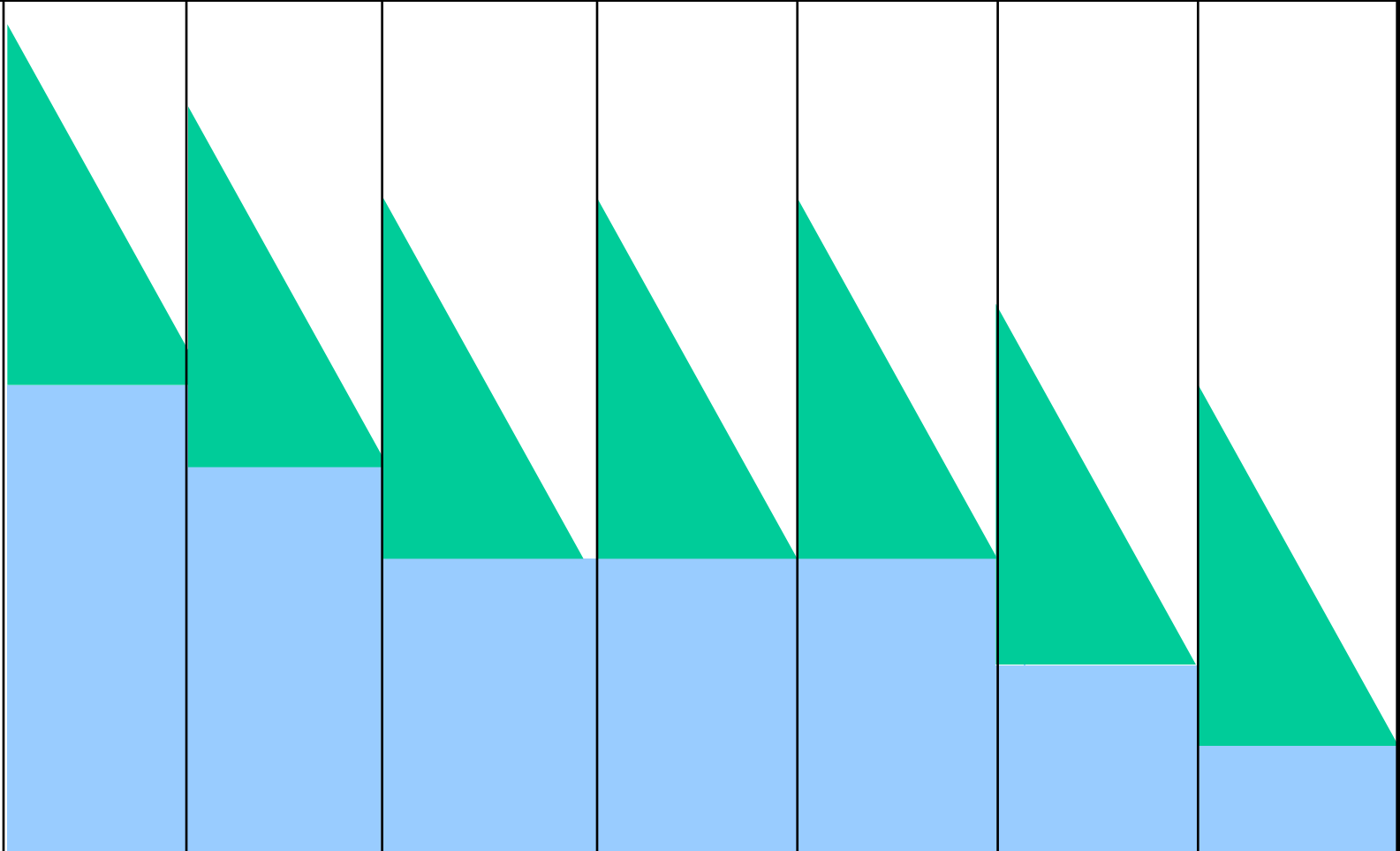
The IT Infrastructure... Is More Than Just Hardware and Software

IT Architecture/ Standards	Human IT Infrastructure	Communications Infrastructure	IT Components	IT Enabled Intangibles	Shared / Standard Applications	Shared IT Services
<ul style="list-style-type: none"> •IS architecture •E-Business architecture •Platform architecture •Standards 	<ul style="list-style-type: none"> •IT management •Operations •Network administration •Communications management •Web administration •Compliance/Assurance interface •Security administration 	<ul style="list-style-type: none"> •Transport management utilities •Network and communication technologies, devices and protocols 	<ul style="list-style-type: none"> •Facilities •Web servers •Application servers •Data/transaction servers •Storage management •UPS •Router/firewall •System software •Data 	<ul style="list-style-type: none"> •Know-how •Corporate culture •Corporate reputation •Environmental orientation •Customer orientation •Knowledge assets or intellectual capital •Synergy •Time •Motivation 	<ul style="list-style-type: none"> •IS processes •Core data processing applications •Shared application systems •Database infrastructure •Web services architecture •Utilities (mail, anti-virus, etc.) 	<ul style="list-style-type: none"> •Service support •Service delivery •Application management •Data management •Channel management •IT R&D •IT training & education •Content management •Knowledge management •Collaboration •User experience and relationship management



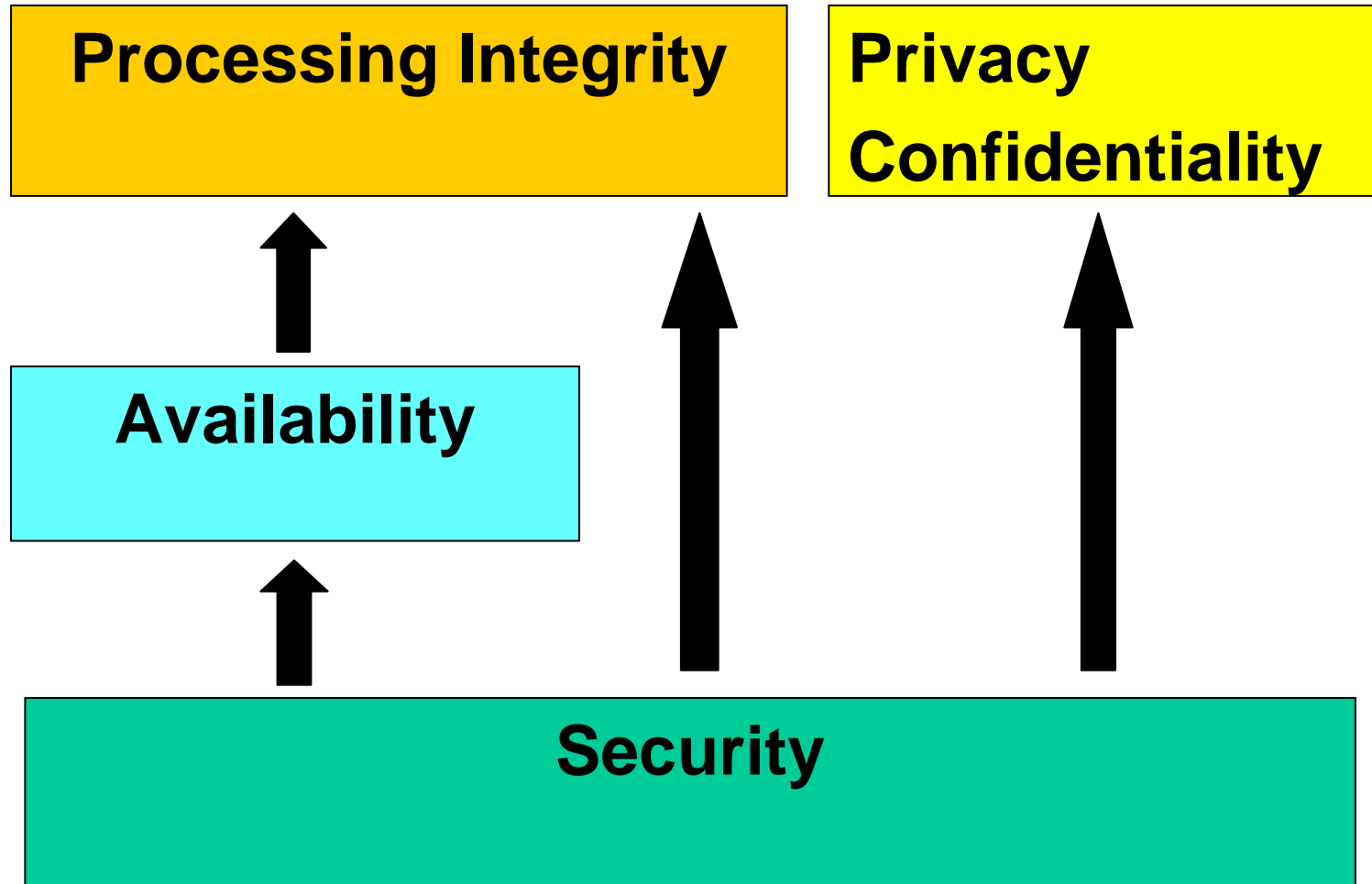
E-Commerce Risk	E-Commerce Risk	E-Commerce Risk	E-Commerce Risk	E-Commerce Risk	E-Commerce Risk	E-Commerce Risk	E-Commerce Risk
H I G H → L O W	H I G H → L O W	H I G H → L O W	H I G H → L O W	H I G H → L O W	H I G H → L O W	H I G H → L O W	H I G H → L O W

Very High ↑
Low ↓



IT Architecture/ Standards	Human IT Infrastructure	Communications Infrastructure	IT Components	IT Enabled Intangibles	Shared/ Standard Applications	Shared IT Services
----------------------------	-------------------------	-------------------------------	---------------	------------------------	-------------------------------	--------------------

Security is the Foundation



Security Program

COSO
ISACA COBIT
CICA ITCG
AICPA/CICA Trust Services
IFAC

ISO 17799/ BS7799
ISO 15408/ Common Criteria
SP800-14&27
FISCAM
GASSP
SSAG
SSE-CMM
CIAO

Components of IT Security Program	COSO	ISACA/ ITGI COBIT	CICA ITCG	AICPA/ CICA Trust Services	IFAC	ISO17799/ BS7799	ISO 15408/ Common Criteria	SP800- 14&27	FISCAM	GASSP	SSAG	SSE-CMM	CIAO- Vulnera- bility Audit Question- naire
Environment/ System Boundary Definition		√		√						√			
Security Policies, Standards & Guidelines		√	√	√	√	√	√	√	√	√			√
Asset Classification and Management			√			√	√		√	√			
Risk Assessment and Cost-Benefit Analysis	√	√	√		√	√		√	√	√	√	√	√
Responsibility and Accountability		√	√	√	√	√	√	√		√	√		√
Personnel Qualifications and Trustworthiness		√	√	√		√		√			√	√	√
Information and Communication/ Security Awareness	√	√	√	√		√				√	√	√	√
User Access Requirements Analysis/ Privilege Management		√	√	√			√	√	√		√		√
Physical Access		√	√	√	√	√	√	√	√		√		√
Logical Access		√	√	√	√	√	√	√	√	√	√		√
Operations Vulnerability Management		√	√	√		√		√			√	√	
Intrusion Detection/ Incident Response		√	√	√	√	√	√	√					√
SDLC Maturity/ Quality		√	√	√		√	√	√		√		√	
Maintenance and Change Management		√	√	√		√							√
Business Continuity		√	√	√		√	√	√	√		√		√
Insurance		√	√	√		√	√	√	√		√		√
Procedural Compliance and Auditability		√	√	√	√	√	√	√			√		√
Monitoring & Learning	√	√	√	√	√	√		√	√	√		√	

Security Program

Security Framework

- **Environment and System Boundary Definition**
- **Security Policies and Standards**

Risk Assessment

- **Asset Classification and Management**
- **Risk Assessment and Cost-Benefit Analysis**

Human Resource Management

- **Responsibility and Accountability**
- **Personnel Qualifications and Trustworthiness**
- **Information and Communication/Awareness**

Access Control

- **User Access Requirements Analysis and Privilege Management**
- **Physical Access Controls**
- **Communications Controls**
- **Logical Access Controls**

Operations and Vulnerability Management

- **Vulnerability Management**
- **Intrusion Detection and Incident Response**

System Acquisition/Development, Maintenance and Change

- **SDLC Maturity/ Quality**
- **Maintenance and Change Management**

Availability and Continuity

- **Physical Availability Controls**
- **Business Continuity**
- **Insurance**

Compliance Monitoring

- **Auditability**
- **Procedural Compliance Verification**
- **Monitoring and Learning**

FOCUS GROUP DEMOGRAPHIC INFORMATION

Gender	
Male	11
Female	1

Employment Information	
Years working experience	
0 to 15	4
16 to 30	6
31 or more	2

Years at most recent or current position	
2 years or less	6
2 to 4 years	3
5 years or more	3

Industry of Current Employer	
Transportation, Communications, Electric	1
Government	1
Education	1
Public Accounting	2
Consulting	3
Finance, Insurance, and Real Estate	4
	12

Current Employment Area	
General Management	1
Information Systems	8
Audit and/or Security	
Consulting	2
Education	1

Number of Employees in Firm	
1 – 100	2
100 – 1,000	2
1,000 – 10,000	4
10,000 – 50,000	3
50,000 – 100,000	1

Education	
College Major	
Accounting	2
Economics	3
Mathematics	2
Information Systems	2
Accounting/IS	1
Arts	1
Marketing	1

Undergraduate Degree	
Arts	5
Commerce/Business	2
Engineering/IT	2
Other	3

Graduate Degree	
MBA, MA	1
MA (Math)	1
None	10

Designations	
CA, CISA	2
CGA, CISA	2
CISA Only	2
CISA/CISM	1
CISA, FLMI	1
CISSP	1
None	3

	IT Infrastructure Components						
Security Elements	IT Architecture and Standards	Human IT Infrastructure	Communication s Infrastructure	IT Components	IT Enabled Intangibles	Shared and Standard Applications	Shared IT Services
Environment and System Boundary Definition	7	4	7	7	3	6	6
Security Policies and Standards	8	8	8	6	6	8	8
Asset Classification and Management	7	5	5	6	4	6	6
Risk Assessment and Cost-Benefit Analysis	8	6	6	6	5	6	6
Responsibility and Accountability	7	9	6	5	6	8	8
Personnel Qualifications	6	8	7	5	7	6	8
Information and Communication/ Security Awareness	5	8	4	4	6	4	5
User Access Requirements Analysis/ Privilege Management	7	7	5	6	4	6	6
Physical Access	6	5	8	8	3	7	8
Logical Access	6	7	7	7	3	8	8
Operations and Vulnerability Management	6	7	8	7	4	8	8
SDLC Maturity/Quality	7	5	5	5	3	7	6
Maintenance and Change Management	6	6	8	8	4	8	8
Business Continuity	5	6	8	8	5	8	8
Insurance	3	2	4	4	1	5	5
Procedural Compliance and Auditability	6	7	6	6	5	7	8
Monitoring and Learning	4	7	5	5	5	6	6

	IT Infrastructure Components						
Security Elements	IT Architecture and Standards	Human IT Infrastructure	Communication s Infrastructure	IT Components	IT Enabled Intangibles	Shared and Standard Applications	Shared IT Services
Environment and System Boundary Definition	10	10	8	10	10	6	10
Security Policies and Standards	10	4	7	10	8	7	10
Asset Classification and Management				1	9	8	8
Risk Assessment and Cost-Benefit Analysis	9			8			
Responsibility and Accountability			5	7		9	9
Personnel Qualifications			10	9	10	6	
Information and Communication/Awareness				4	9	9	8
User Access Requirements Analysis/ Privilege Management	8		9	8	9	9	9
Physical Access	10		10	6		10	10
Logical Access	8		8	7		6	10
Operations and Vulnerability Management	10	10	5	8	9		
SDLC Maturity/Quality	9	10	7	7	10	8	
Maintenance and Change Management	10	10	10	7	10	8	10
Business Continuity	5		5	5		9	8
Insurance	8						
Procedural Compliance and Auditability	10		9	6	9	7	9
Monitoring and Learning	8						

SUMMARY OF SECURITY ISSUES DISCUSSED IN THE SECURITY LITERATURE

Security-related articles that appeared from 2001 to 2005 in the following professional and academic publications were read and summarized:

- *SC Magazine*,
- *Information Systems Control Journal*,
- *Security Journal*,
- *Communications of the ACM*,
- *Computerworld* and
- *Computing Canada*.

Appendix summarizes the key points discussed in these sources.

Research Issues

- Is this our territory?

Research Issues: What is unknown?

- Objective evidence about basic facts
- Quality of frameworks
- Consequences of failures
- People issues
- Systems/Organizations/Sector issues
- Interactions

Research Issues: What is unknown?

- Objective evidence about basic facts
 - Frequencies, costs, benefits

Research Issues: What is unknown?

- Quality of frameworks
 - Completeness
 - Usefulness

Research Issues: What is unknown?

- Consequences of failures –
 - outages,
 - disclosures,
 - errors,
 - identity theft

Research Issues: What is unknown?

- People
 - Hackers - Attack strategies, incentives
 - Ethical hackers – knowledge, heuristics, etc.
 - Anti-hackers
 - Defense strategies – individual, organizational, societal
 - Design strategies
 - Testing strategies
 - Users
 - Trust
 - Knowledge, incentives

Research Issues: What is unknown?

- Systems/Organizations/Sectors
 - Configurations
 - Organizations
 - Incentives for “compliance” by employees – punishment vs. training
 - Internal auditors vs. security pros – turf wars, world views
 - Penalties for producers of flawed software – limits to foreseeability
 - Processes for incorporating best practices
 - Secretive vs. open organizations – least privilege vs. max privilege

Research Issues: What is unknown?

- Interactions
 - Hackers vs. Anti-Hackers
 - People vs. Systems
 - People vs. Organizations

Research Issues: What is unknown?

- Objective evidence about basic facts
 - Frequencies, costs, benefits
- Quality of frameworks
 - Completeness
 - Usefulness
- Consequences of failures – outages, disclosures, errors, identity theft
- People
 - Hackers - Attack strategies, incentives
 - Ethical hackers – knowledge, heuristics, etc.
 - Anti-hackers
 - Defense strategies – individual, organizational, societal
 - Design strategies
 - Testing strategies
 - Users
 - Trust
 - Knowledge, incentives
- Systems/Organizations/Sectors
 - Configurations
 - Organizations
 - Incentives for “compliance” by employees – punishment vs. training
 - Internal auditors vs. security pros – turf wars, world views
 - Penalties for producers of flawed software – limits to foreseeability
 - Processes for incorporating best practices
 - Secretive vs. open organizations – least privilege vs. max privilege
- Interactions
 - Hackers vs. Anti-Hackers
 - People vs. Systems
 - People vs. Organizations

Research Issues

Q&A