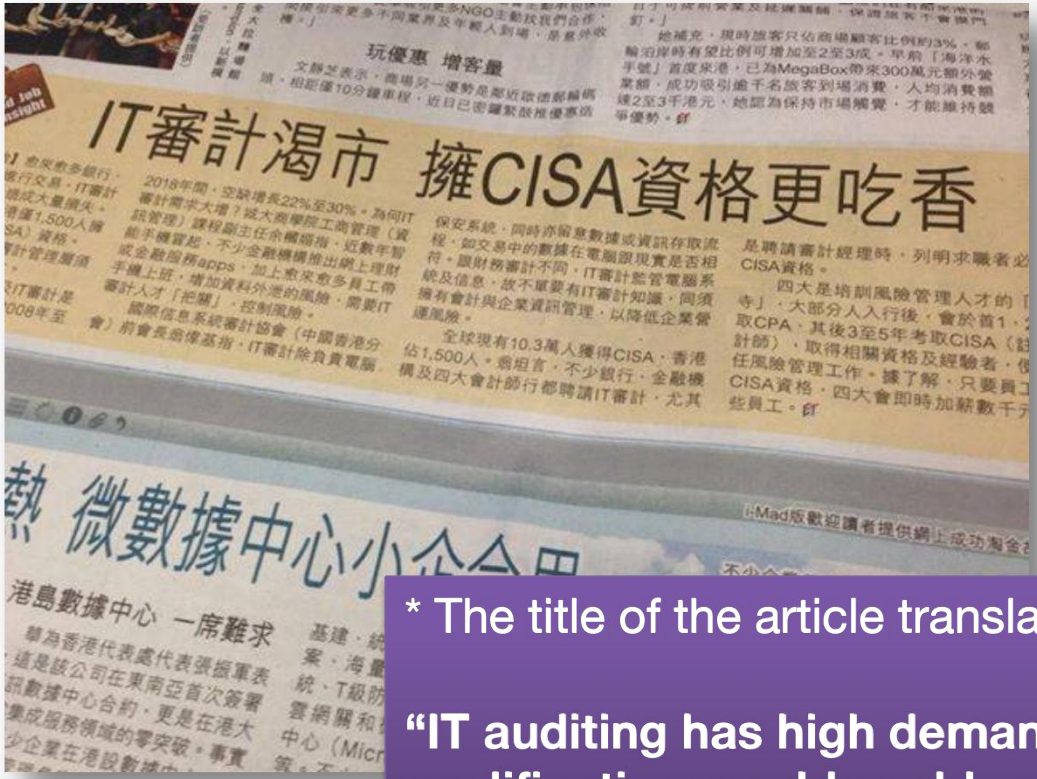
Week 9: Smart Accounting; Information Security Management; Business Continuity Planning

CB2500 Information Management

Smart Banking (BI)
Smart e-Services (ISSN)

Smart IS Auditing (ISA)
Smart Global Business (GBSM)

What are the roles of IS employees in risk management and IS/IT auditing areas?



* The title of the article translates to:

“IT auditing has high demand, CISA qualification would enable you to be more competitive”

"What are the new auditing and consultancy services we should provide to our clients?"

- What are the business trends related to audit firms and risk management?

Deloitte.

ERNST & YOUNG

KPMG

pwc

Study Questions / Intended Learning Outcomes

QX1: What are the roles of IS staff in risk management and IS/IT auditing areas?

Q10-1: What is the goal of information systems security?

Q10-5: How can technical safeguards protect against security threats?

Q10-6: How can data safeguards protect against security threats?

Q10-7: How can human safeguards protect against security threats?

QX2: What is business continuity planning?

QX3: What is (Information) Ethics?

QX4: What are the policies companies could adopt?

QX1: **What are the roles of IS staff in risk management and IS/IT auditing areas?**

- IT/IS Auditing: what they are NOT
  - Accounting control/financial auditing
  - Compliance testing
  - Out of scope

Reference: https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basicsthe-core-of-it-auditing

Challenges to Corporate Governance

- What is Corporate Governance?
  - A collection of mechanisms and processes to control and operate a firm

- Challenges to Corporate Governance
  - Bring Your Own Device (BYOD)
  - Data Proliferation
  - Privacy

COBIT

- COBIT
  - Control Objectives for Information & Related Technologies
  - A framework designed by ISACA
    - Information Systems Audit and Control Association
  - A reference framework for professionals to help companies to manage risks related to the use of information systems

It's about operational risk management

BUSINESS GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Download a complimentary copy of COBIT 5 today or learn more at
www.isaca.org/cobit

COBIT 5

AN ISACA® FRAMEWORK

Not to be covered in CB2500, but in other IS courses, e.g.

1. IS4537 Information Systems Audit
2. IS4435 Governance & Regulatory Compliance for Financial Information Systems
3. IS4543 Risk Management and Information Systems Control

Technology Risk Management - Manager

Bank of China (Hong Kong) Limited

Central

- Conduct regular onsite IT Risk assessment
- Act as a Subject Matter Expert
- Medical and life insurance

18-Mar-20

ambition

IT Audit, Manager

Ambition

HK$30k - 55k /month (negotiable)

- Commercial Corporate Banking Group
- CISA, CISSP
- Attractive salary package

17-Mar-20

HSBC

GBM IT Audit Manager - Global Internal Audit

HSBC Group

Other Locations

- One of the world's leading international banks
- Excellent Career Progression
- Dynamic working environment

17-Mar-20

Get job alerts for this search Subscribe

Apply Now View in new tab Clos

transparent operation of financial markets.

The ideal candidate for this role will have:

- Excellent spoken and written communication skills with experience of adapting your style and approach to the audience and message to be delivered.
- Solid understanding of risks and controls, and role of first, second and third line of defence.
- Availability to travel to regional offices when required, however this is not expected to be significant.
- A track record of gaining an understanding of customers' needs and delivering excellent customer service.
- A track record of constantly looking for ways to do things better and an excellent understanding of the mechanism necessary to successfully implement change.

The following are beneficial to have, but not mandatory:

- Relevant experience working in Investment Banking or Financial Services, including having a solid understanding of financial products and services.
- Past experience working in an Audit or Risk based role, e.g. Internal / External Auditor, Risk Steward, Control Officer.
- Role relevant qualifications, e.g. Certified Information Systems Auditor (CISA).

You'll achieve more when you join HSBC.

www.hsbc.com/careers

HSBC is committed to building a culture where all employees are valued, respected and opinions count. We take pride in providing a workplace that fosters continuous professional development, flexible working and opportunities to grow within an inclusive and diverse environment. Personal data held by the Bank relating to employment applications will be used in accordance with our Privacy Statement, which is available on our website.

How to be an IS Auditor

- Professional qualification: CISA
  - Certified Information Systems Auditor
- CISA Exam
- Maintaining CISA certification
  - Continuing professional education (CPE)
  - Annual maintenance fee
  - Random selection of annual CPE audit

CISA Certified Information Systems Auditor
An ISACA Certification

How to be an IS Auditor

- To certify, you need:
  - Passing the CISA exam (covering 5 domains)
  - Five years work experience in the fields of Information Systems Auditing, Control, Assurance or Security
  - Work experience waiver is available

Universities with ISACA Enriched Curriculum

Hong Kong

City University of Hong Kong, College of Business, www.cb.cityu.edu.hk/is/programmes/bachelor/BBAIM/ISA/,
Bachelor of Business Administration in Information Management [BBAIM]—Information Systems Auditing stream
Contact: **Dr. Terence Cheung**, Assistant Professor and Programme Leader of BBAIM, is.tc@cityu.edu.hk or +852 3442 2303.

Hong Kong University of Science and Technology, www.ust.hk, www.bm.ust.hk/isom
Bachelor of Business Administration in Information Systems [BBA(IS)].
Contact: **Dr. Garvin Percy DIAS**, Associate Professor of Business Education (IS Undergraduate Coordinator), Department of Information Systems, Business Statistics and Operations Management, percy@ust.hk.

Hong Kong Baptist University, School of Business www.hkbu.edu.hk/~bba/isem.php
Bachelor of Business Administration (honors) in Information Systems and e-Business Management [BBA(ISEM)]
Contact: **Dr. Tony C.K. Wong**, Coordinator, BBA (Hons) Information Systems and e-Business Management Concentration Department of Finance and Decision Sciences, tckwong@hkbu.edu.hk or +852 3411-7580

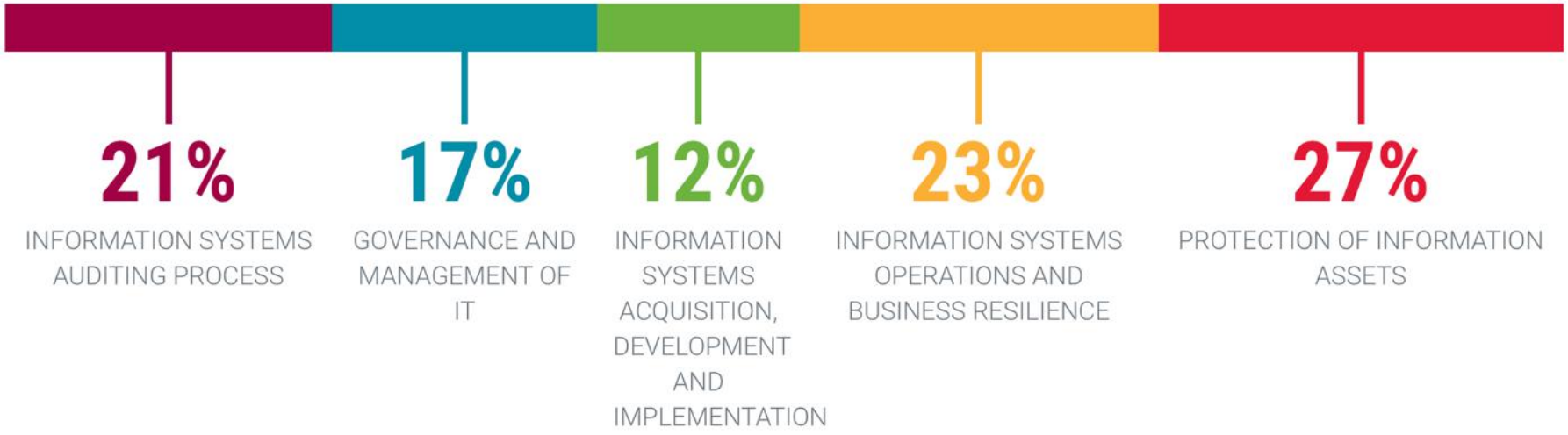
The University of Hong Kong, www.business.hku.hk/bbaIS.html ,
Bachelor of Business Administration (Information Systems) [BBA(IS)].
Contact: **Dr. Michael Chau**, Associate Professor, Bachelor of Business Administration (Information Systems) and Bachelor of Engineering (Computer Science) Programs Coordinator, Faculty of Business and Economics, mchau@business.hku.hk.

Link: https://www.isaca.org/membership/model-curricula
Please note: ISACA's Model Curricula program is currently on hold and at this time ISACA are not accepting any new applications for recognition.

5 Domains in CISA

THE CISA DIFFERENCE

Whether you are seeking a new career opportunity or striving to grow within your current organization, a CISA certification proves your expertise in these work-related domains:

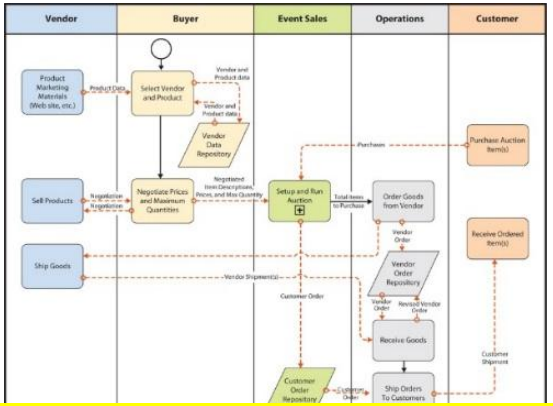


Source: https://www.isaca.org/credentialing/cisa/cisa-job-practice-areas

Domain 1. Information Systems Auditing Process

- Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems.

- Knowledge / skills needed, e.g.
  - Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits
  - Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT



knowledge and skills (law, business process, systems) in providing IS audit services

Domain 2. Governance and Management of IT

- Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy.

- Knowledge / skills needed, e.g.
  - Knowledge of enterprise risk management
  - Knowledge of business impact analysis (BIA) related to business continuity planning

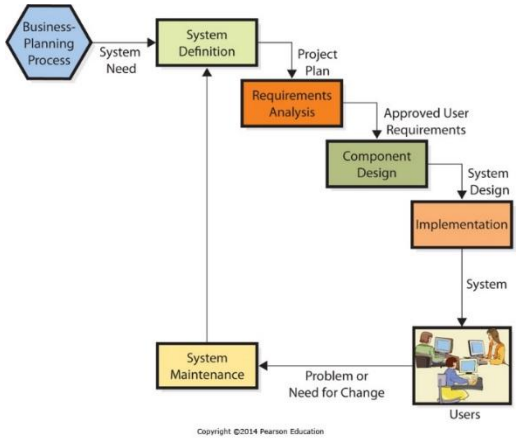
mgmt's view point of risk mgmt

** http://youtu.be/cxE940f7iq0
http://youtu.be/d60m6hUpgys

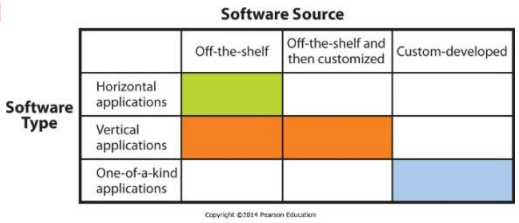
mgmt + org structure + process ← are they available in the company to align IT with company's strategy?

Domain 3. Information Systems Acquisition, Development and Implementation

- Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.



- Knowledge / skills needed, e.g.
  - Knowledge of acquisition practices
    - Horizontal/vertical/one-of-a-kind, open source, etc?
  - Knowledge of system development methodologies, e.g. SDLC



acquiring/implementing new systems ← any mistake?

Domain 4. Information Systems Operations and Business Resilience

- Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

- Knowledge / skills needed, e.g.
  - Knowledge of systems performance monitoring processes
  - Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery

Daily operation + support of systems ← ok?
e.g. license management, insurance of HW

Domain 5. Protection of Information Assets

- Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

- Knowledge / skills needed, e.g.
  - Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
  - Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets


Mirror NEWS
Real news, real enterta
FRONT PAGE | NEWS | SPORT | 3AM | TV | LIFESTYLE | MONEY
News · Technology & Science · Technology · Crime
By Chris Richards | Comments | 4 Oct 2013 01:56
Crooks hack into Adobe and steal personal data of 2.9 MILLION users
The credit and debit card numbers of many customers have fallen into the hands of the hackers, sparking a police investigation
25 Like 68 Send
Crooks have hacked into the software company Adobe and stolen the personal data of 2.9 million users.
The US firm, which makes Photoshop and other programs, revealed that cyber attackers had accessed user information, including account IDs and encrypted passwords as well as credit and debit card numbers.
The hackers were able to erase some Adobe users' data .

info assets' protection, storage, disposal, etc ← ok?

Q10-1: What is the goal of information systems security?

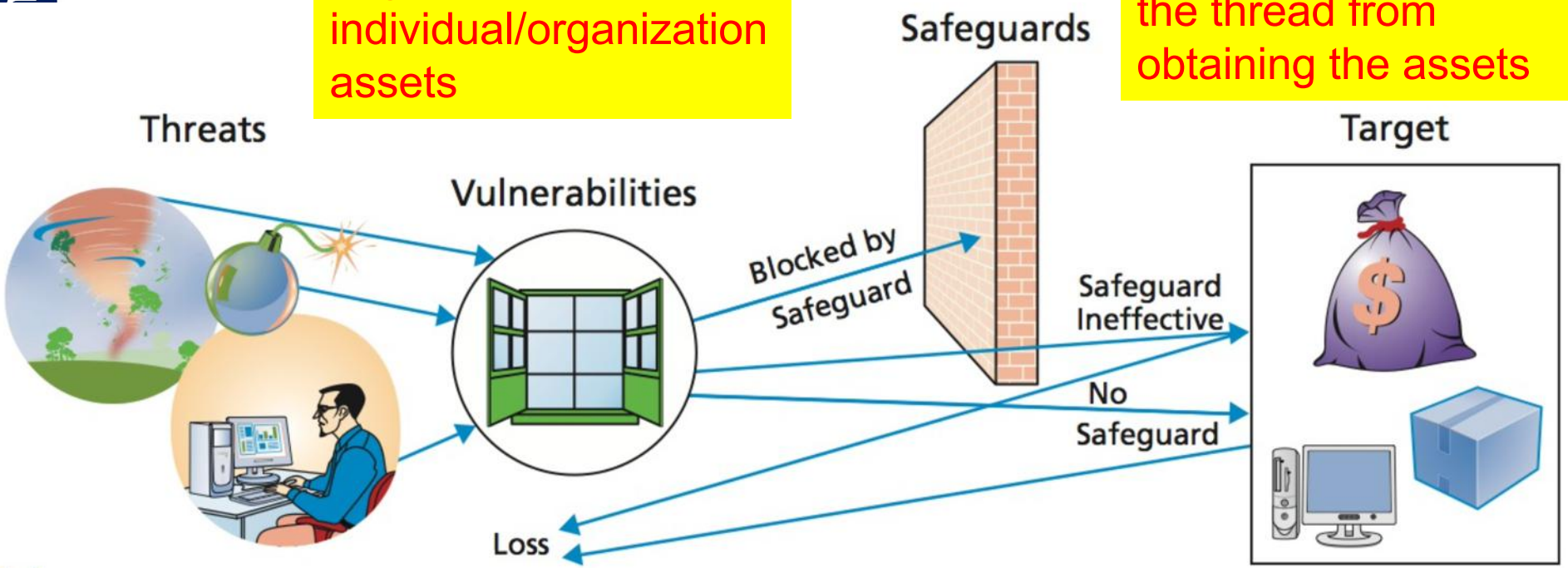
Cost

Risk

Elements of Threat/Loss

opportunity for threats to gain access to individual/organization assets

some measure that ind/org take to block the thread from obtaining the assets



Person/org that seeks to obtain/alter data/IS assets illegally

Asset desired by the threat

An example of Threat/Loss scenario

Threat/Target	Vulnerability	Safeguard	Result	Explanation
Hacker wants to steal your bank login credentials	Hacker creates a phishing site nearly identical to your online banking site	Only access sites using https	No loss	Effective safeguard
		None	Loss of login credentials	Ineffective safeguard

Sources of Threat

- Human Error

- Computer Crime

- Natural Events and Disasters

What types of security loss are there?

- Unauthorized data disclosure
  - occurs when a threat obtains data that is supposed to be protected

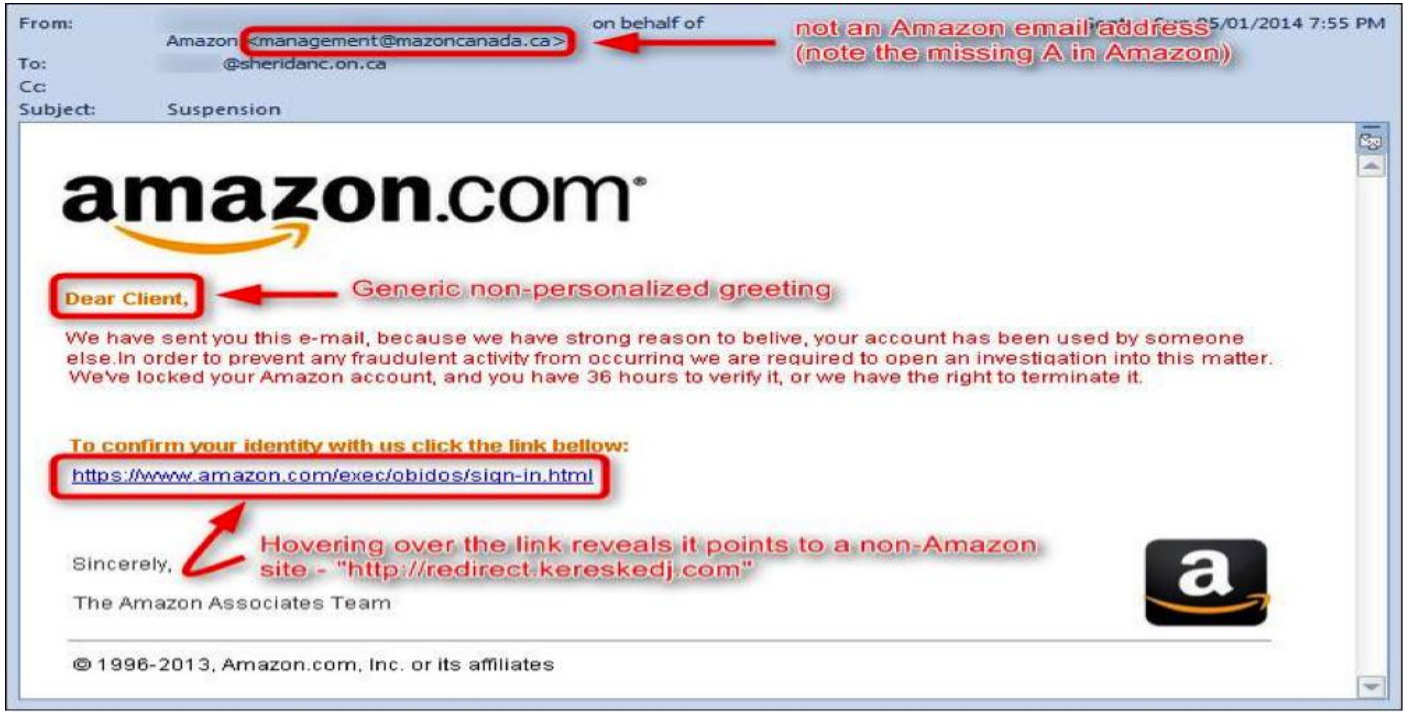
What types of security loss are there?

- Pretexting: pretending to be someone else
- Spoofing:
  - IP sniffing
  - Email sniffing: Phishing
- Sniffing: intercepting computer communication (e.g., spyware and adware)
- Hacking: break into computers/servers/networks

What types of security loss are there?

- Unauthorized data disclosure
  - Pretexting: pretending to be someone else
  - Phishing
  - Sniffing
  - Hacking

Phishing Email



What types of security loss are there?

- Incorrect data modification
  - Typos
  - Computer hacking

An 11-year-old changed election results on a replica Florida state website in under 10 minutes

Nation Aug 12, 2018 5:00 PM EDT

An 11-year-old boy on Friday was able to hack into a replica of the Florida state election website and change voting results found there in under 10 minutes during the world's largest yearly hacking convention, DEFCON 26, organizers of the event said.

What types of security loss are there?

- Faulty service: problems due to incorrect system operations
  - Could overlap with incorrect data modification
  - A specific type: Usurpation

Usurpation:
when hackers invade a computer system and replace legitimate programs with their own authorized ones that shut down legitimate apps and substitute their own processing to spy/manipulate

What types of security loss are there?

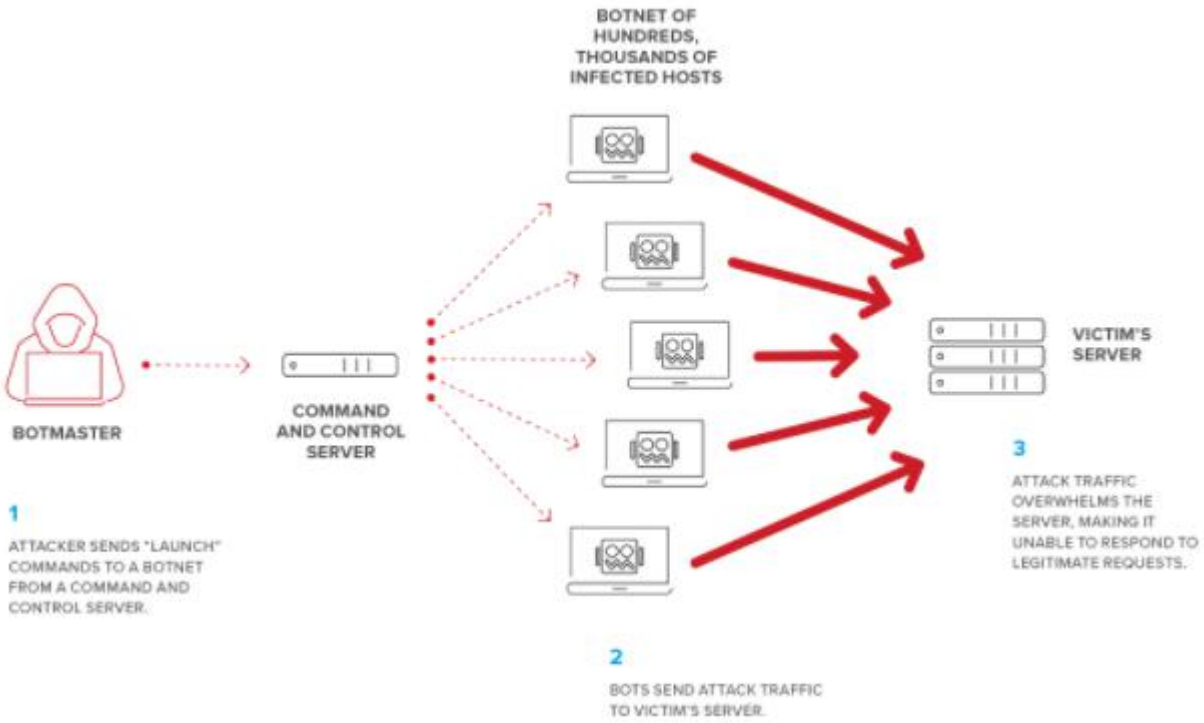
- Denial of service (DoS)

- A type of attack on a service that disrupts its normal function and prevents other users from accessing it

What types of security loss are there?

- Distributed denial-of-service attack (DDoS attack)

Denial-of-service and Distributed Denial-of-service Attacks



Threat vs. Loss: A summary

		Threat		
		Human Error	**Computer Crime**	**Natural Disasters**
Loss	**Unauthorized data disclosure**	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Hacking	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Usurpation	Service improperly restored
	Denial of service (DoS)	Accidents	DoS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

Safeguards Against Security Threats?

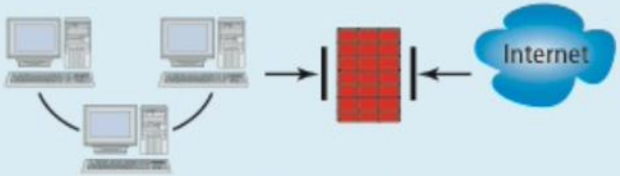
Identification and authorization	Data rights and responsibilities	Hiring
Encryption	Passwords	Training
Firewalls	Encryption	Education
Malware protection	Backup and recovery	Procedure design
Application design	Physical security	Administration
		Assessment
		Compliance
		Accountability

Q10-5: How Can Technical Safeguards Protect Against Security Threats?

- Identification and authentication

- Encryption

- Firewalls



- Malware protection

Identification & authentication

- Username: identification
  - E.g., EID
- Password: authentication

- Weakness?

Identification & authentication

- How to deal with weakness? What are the alternatives to username & password?

Encryption

- Encryption is the process of transforming clear text into coded, unintelligible text for secure storage or communication.

- Key: a string of bits to encrypt data

Encryption: Example with Advanced Encryption Standard (AES)

- An online tool: https://aesencryption.net
- Encrypted message:
  - "gxVfaeEYf7K6y8W7v2HTuA=="
- Key: "yes"

- What is this message?

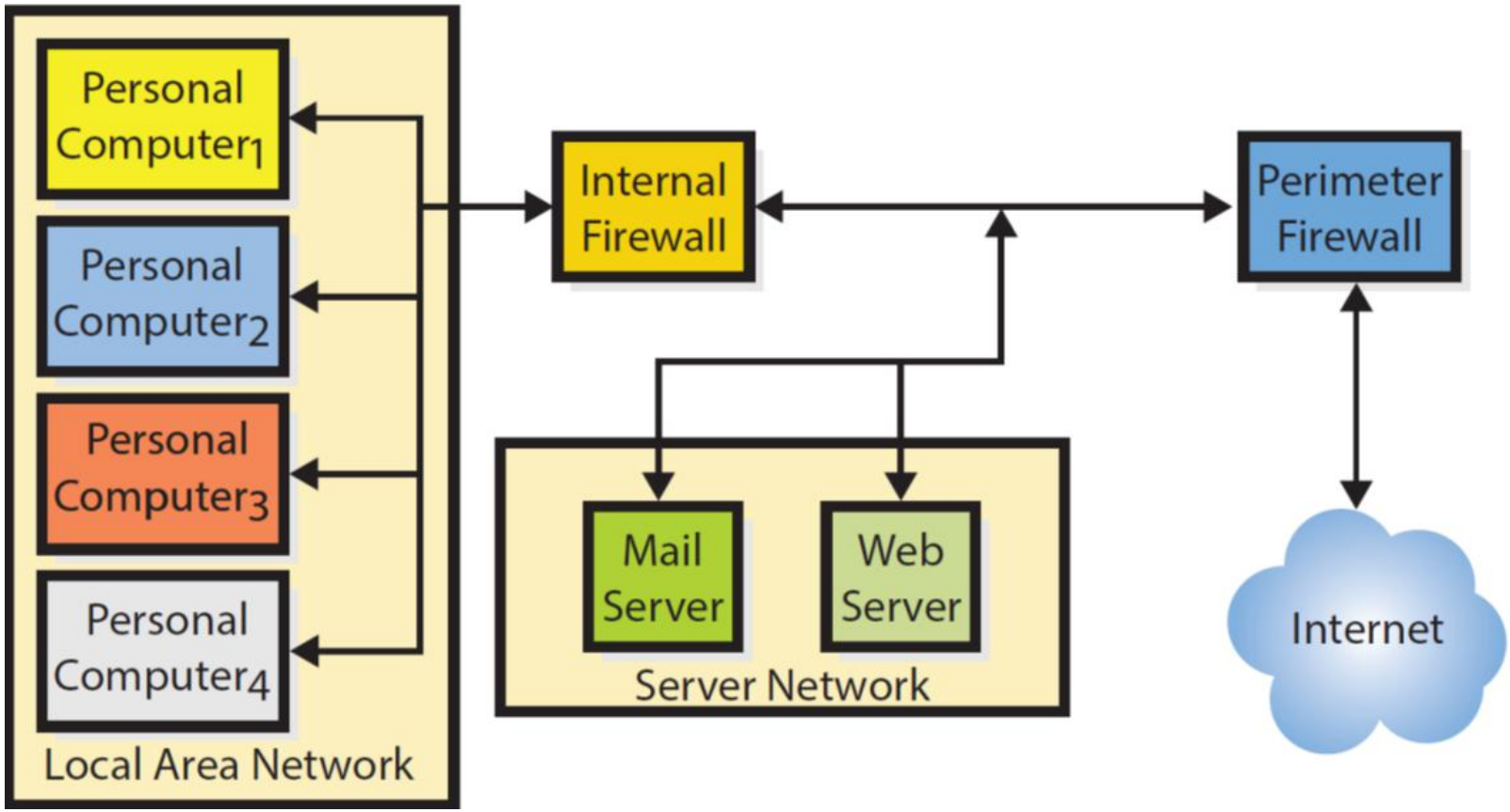
Asymmetric & Symmetric Encryption

- Symmetric: the same key for both encryption and decryption

Asymmetric & Symmetric Encryption

- Asymmetric: separate keys.
  - Public key encryption:
    - Public key for encryption (or, ”lock” the message”)
    - Private key for decryption (or, “unlock”)

Firewalls


Personal Computer1
Personal Computer2
Personal Computer3
Personal Computer4
Local Area Network
Internal Firewall
Perimeter Firewall
Mail Server
Web Server
Server Network
Internet

Malware protection

- Malware: viruses, spyware, adware, and worms etc.

Malware protection

- Malware: A broad category of software including
  - Viruses: computer programs that _____
  - Spyware: resides in the backgro
  - _____
  - Adware: mostly harmless but produce popup ads

Q10-6: How Can Data Safeguards Protect Against Security Threats?

- What do data safeguards protect?

Q10-6: How Can Data Safeguards Protect Against Security Threats?

What organization units are responsible?

- _____: refers to an organization-wide function that oversees developing data policies and enforcing data standards.

- _____:
  - Refers to a function that pertains to a particular database.
  - ERP, CRM, and MRP databases each have this function.

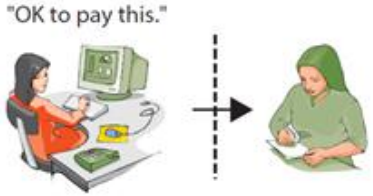
Q10-6: How Can Data Safeguards Protect Against Security Threats?

- Define data policies
- Data rights and responsibilities
- Rights enforced by user accounts authenticated by passwords
- Data encryption
- Backup and recovery procedures
- Physical security

What're the roles of IS professions such as IS auditors?

Q10-7: How can Human Safeguards Protect Against Security Threats?

- Position definition
  - Separate duties and authorities
  - Determine least privilege
  - Document position sensitivity



- Hiring and screening

- Dissemination and enforcement
  - responsibility
  - accountability
  - compliance

- Termination
  - Friendly

  - Unfriendly

What should companies do to minimize impact of disastrous events?

And to recover from them?

Business Continuity Plan

Video URL: https://www.youtube.com/watch?v=cxE940f7iq0

QX2: What is business continuity planning?

- To enable a business to continue offering critical services in the event of a disruption
- To survive a disastrous interruption to activities.
- Rigorous planning and commitment of resources is necessary to adequately plan for such an event.

So, an IS auditor has to:
1. Identify critical services a company should continue to offer after interruption (resources? regulation? → e.g. what is a bank's critical service? What are the resources needed? Any regulations banks have to follow?)

QX2: What is business continuity planning?

- To enable a business to continue offering critical services in the event of a disruption
- To survive a disastrous interruption to activities.
- Rigorous planning and commitment of resources is necessary to adequately plan for such an event.

So, an IS auditor has to:
2. Help planning for resources and procedure for recovering your client's business in the shortest possible time. (e.g. any back up site / facilities / data? Procedure? Employees?)

Disasters and Other Disruptive Events

- Natural disasters
  - Earthquakes, floods, tornados, severe thunderstorms, fire, …
- Other disastrous events
  - Outrage of electricity, telecommunication service, gas supply, …
  - Or terrorist attacks, hacker attacks, viruses or human error
  - System malfunctions, accidental file deletions, untested application release, loss of backup, DoS attacks,…

Implication towards data center's site selection?

Disasters and Other Disruptive Events

- Natural disasters
  - Earthquakes, floods, tornados, severe thunderstorms, fire, …
- Other disastrous events
  - Outrage of electricity, telecommunication service, gas supply, …
  - Or terrorist attacks, hacker attacks, viruses or human error
  - System malfunctions, accidental file deletions, untested application release, loss of backup, DoS attacks

Implication towards data center's site selection:
A location that's far away from natural disasters, reliable and steady power supply, low crime rate, no interference of data flow in/out.

IS Auditor's Tasks

- Reviewing BCP
- Reviewing BC teams
- Evaluating prior test results
- Evaluating offsite storage
- Interviewing key personnel
- Evaluating security at offsite facility
- Reviewing alternative processing contract
- Reviewing insurance coverage

Incident Management

Exhibit 2.16—Incident/Crisis Levels

1 LEVEL		MAIN CRITERION (hours) SERVICE DOWNTIME FORECAST > =	ACTUAL > =
CRISIS	7		24
	6	24	12
MAJOR INC'T	5	12	6
	4	6	4
	3	4	2
MINOR INC'T	2	2	1
	1	1	0.5
NEGLIGIBLE	0		

COMPLEMENTARY CRITERIA	
DATA	PLATFORMS
Database loss of integrity	Hacked or Denial of Service Attack
	Viruses, worms. Hardware failure.
Lost transactions	

LEVEL		2 ACTIONS	
CRISIS	7	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies
	6	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies
MAJOR	5	Prepare for Business Continuity Plan	Alert SM
	4	Correct/Clean/Restore/Replace	Alert SM
	3	Correct	If confirmed, alert SO
MINOR	2	Correct	
	1	Correct	
NEGLIGIBLE	0	Log	(Analyze logs regularly)

SM = Senior Management
SO = Security Officer

Alerting Key Decision-making Personnel in BCP

- Telephone list / "call tree"
  - A notification directory, of key decision-making IS and end-user personnel required to initiate and carry out recovery efforts
- Should contain:
  - A prioritized list of contacts
  - Contacts of each critical contact person (usually key team leaders)
  - Contacts of representatives of equipment and software vendors, recovery facilities, media storage facilities, insurance company agents, HR services, legal/regulatory/governmental agencies
  - A procedure to ascertain how many people were reached while using the call tree

BCPs in action: Challenge from COVID-19

Video URL: https://www.youtube.com/watch?v=yjMrwVMAVrA

UReply Q1

Based on the video:

1. **What are companies' BCPs in face of COVID-19 and the need of social distancing?**

2. **What are the challenges/downsides?**

CB2500 Information Management

Smart Banking (BI)
Smart e-Services (ISSN)

Smart IS Auditing (ISA)
Smart Global Business (GBSM)

QX3: What is (Information) Ethics?

- It governs the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution, and processing of information itself

- Ethical issues in the areas of copyright infringement and intellectual property are affecting

IT makes ethics a bigger issue to handle, why?

What is Information Ethics?

- Technology makes it easy to copy everything digital!

As a result, several technology-related issues arise!

Intellectual Property	Intangible creative work that is embodied in physical form
Copyright	The legal protection afforded an expression of an idea
Fair Use Doctrine	In certain situations, its legal to use copyrighted material
Pirated Software	Unauthorized use, duplication, distribution, or sale of copyrighted software
Counterfeit Software	Software that is manufactured to look like the real thing and sold as such

Everything's faster, easier, and more globalized, e.g.
- it is easy to download tools to hack a company website
- downloading and sharing pirated software

What can be done?

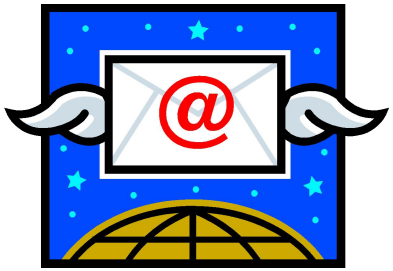
- Governments should implement and enforce laws related to information ethics (privacy)

- The Hong Kong Government through the Office of the Privacy Commissioner for Personal Data (PCPD) aims to secure the protection of privacy of the individual with respect to personal data through promotion, monitoring and supervision of compliance with the Personal Data (Privacy) Ordinance.
- http://www.pcpd.org.hk/

Government setting up laws, e.g. http://www.pcpd.org.hk/english/resources_centre/multimedia/video/video.html

QX4: What are the policies companies could adopt?

- Organizations can consider adopting the following policies
  - Ethical computer use policy
  - Acceptable use policy
  - Email privacy policy



Email Privacy Policy

- It details the extent to which email messages may be read by others
- To a large extent, user's expectation of privacy is based on the false assumption that email privacy protection exists, i.e. no one else can read his/her emails
- However, large organizations regularly read and analyze employees' email looking for confidential data leaks
- Hence, email privacy policy is usually spelt out to every employee

Employers may "read" employee's emails → prevent confidential data leaks;
if no Email Privacy Policy but employer reads employee's email → problem

Email Privacy Policy

- A typical email privacy policy also defines, among others,
- Discourages users from sending junk email or spam to anyone who does not want to receive it
- Informs users that the organization has no control over email once it has been sent out
- Explains what happens to accounts after a person leaves the organization

No spamming; responsibility issue

Why is this lecture valuable to you?

- This lecture prepares you to become an IS auditor.
- You need to domain knowledge of CISA and business continuity planning for risk assessment and preparation against potential operational risks
- You need knowledge in business continuity plans to get prepared for any unexpected events.

Week 9 Recap

QX1: What are the roles of IS staff in risk management and IS/IT auditing areas?

Q10-1: What is the goal of information systems security?

Q10-5: How can technical safeguards protect against security threats?

Q10-6: How can data safeguards protect against security threats?

Q10-7: How can human safeguards protect against security threats?

QX2: What is business continuity planning?

QX3: What is (Information) Ethics?

QX4: What are the policies companies could adopt?

References and Disclaimer

- Ch. 10
- Information Systems Audit and Control Association (www.isaca.org)
- Certified Information Systems Auditor (CISA)
- Reference book (Business Driven Technology, 5th edition) Chapter B7
- Online cases

- The PPT from publisher is slightly modified to suit the teaching/learning pace.
- Photos used in this PPT are copyrighted by the corresponding owners.