國立中央大學資訊管理學系碩士在職專班九十一學年度入學考試

考試科目：資訊管理個案分析 (共二個 Case)

Case 1: **Nabisco Biscuit Company** (50%)

Instruction: Please read the attached case and answer the following four questions. Please write either in English or in Chinese.

1. Please briefly summarize the case in less than 500 words.
2. What problems did Nabisco Biscuit Company face, and what competitive strategy did the company follow to address these problems?
3. What alternatives could the company take to improve the situation? Evaluate both the benefits and shortcomings for each alternative you propose. How could it have better supported the company's strategic goals.
4. What management, organization, and technology issues had to be addressed while making changes.

Case 1:

When Nabisco Biscuit Company launched its SnackWell's Devil's Food Cookie Cakes, it anticipated there might be problems. Convincing people that a fat-free chocolate and marshmallow cookie is not only tasty but good for them is a tall order. But it's what Nabisco didn't anticipate that has customers peeved. The company can't manufacture the cookies fast enough. One lady was reportedly angry enough to chase a delivery truck driver all the way back to a distribution center. Resigned officials have given up trying to furnish explanations and simply urged cookie lovers to try one of Nabisco's other offerings. The company can't make the product fast enough, and no one is happy about it.

Skeptics wonder how an operation that produces 600 million pounds of cookies annually can't just turn up the volume. It turns out that there's more to the process than the average snacker might think. "There is no such thing as a simple cookie," says Brian Beglin, senior director of operations services. "But the Devil's Food Cookie Cake is the hardest one we make." Cookies that aren't coated with chocolate on all sides can be run along a conveyor and deposited into a waiting container. The marshmallow cream center of the Snackwell's cookie gets chocolate all over. It sticks to everything, including conveyor belts.

So Snackwell's cookies are produced through the use of a pin-trolley system, a process that has gone largely unaltered for 70 years. Baked cookies are skewered on a little double-pronged fork. They then make a one-mile trip through the bakery getting doused and dolloped with marshmallow and chocolate and a final glazing. Things don't get any easier after that. The fat-free chocolate covering can't be chilled, which would make the cookies congeal, so the cookies must be air dried. Because of these special requirements, the process takes four hours. By comparison, creating a bag of Chips Ahoy! cookies take 30 minutes from start to finish.

Nabisco acquired the necessary custom-made machinery to make Snackwell's from a Sioux City, South Dakota, bakery owned by Interbake Foods, Inc. That also happens to be the only place the equipment is available. Increasing capacity would be neither easy nor cheap. The company has three production lines running overtime and will soon add another. But that will reportedly do it for the machine-building capacity of the Interbake plant. More cookie production after that will cost the company a lot more money.

Using 1920s-era processes to produce Snackwell's didn't result in a lot of finger-pointing at Nabisco. The company has produced cookies that require the use of the pin-trolley system for many years. The problem, if it can be called that, is that no one expected Snackwell's to be so popular. The key to what made the cookie such a hit may be in the different process that went into making it. By using cocoa instead of chocolate, reducing the fat content wasn't difficult, and the fat-free cookie tastes authentic. Nabisco's big decision is what to do now.

Customers are still clamoring for more product, and it seems inconceivable that they will simply be left standing in line. On the other hand, adding costly capacity could backfire if the fad fades. None of this has escaped competitors. Keebler has launched its own reduced-fat cookie line. Despite racking up over $100 million in sales in just its first year, there are no guarantees about the sometimes fickle sweet tooths of consumers. But no one need shed tears for Nabisco. After all, the company knew that some kind of problem always arises launching a new product.

SOURCES: Kathleen Deveny, "Man Walked on the Moon but Man Can't Make Enough Devil's Food Cookie Cakes," *The Wall Street Journal,* September 28, 1993, I-1, I-2; Julie Liesse, "Sharon Rothstein-Snackwell's," *Advertising Age,* July 5, 1993; Julie Liesse, "Snackwell's Soars at Nabisco," *Advertising Age,* April 5, 1993; and "Cookies Offer Food for Thought—RJR Nabisco," *Financial Times,* August 24, 1993.

Case 2: Canadian Imperial Bank of Commerce (50%)

Read the following Canadian Imperial Bank of Commerce case carefully and then answer the four questions attached at the end of this case either in Chinese or English.

Canadian Imperial Bank of Commerce:

"We could have a lively situation on our hands if some of these e-mail privacy scenarios come true," remarked Bob Jones, manager, Compliance at Canadian Imperial Bank of Commerce (CIBC). It was May 16, 2000, and Jones was aware that Toronto-based CIBC had implemented word recognition software in its U.S. broker to comb e-mail messages sent by employees for specified business words. What if these routine searches flagged an e-mail message that also contained personal information about an employee? In the wake of an e-mail "worm" that crippled corporate networks in the first week of May 2000, use of e-mail at work was a hot topic of discussion in management circles.

Canadian Imperial Bank of Commerce

As of May 2000, Canadian Imperial Bank of Commerce had 45,000 employees worldwide serving six million individual customers, 350,000 small businesses, and 7,000 corporate and investment banking customers. The bank had total assets of $250 billion, and a net income of $1.029 billion in 1999.

Formed out of a 1961 merger between The Canadian Bank of Commerce and Imperial Bank of Canada, CIBC was one of North America's leading financial institutions offering retail and wholesale products and services through its electronic banking network, branches and offices around the world.

Customer Privacy in the Banking Industry: The Tournier Case

Privacy practices in the banking industry could be traced back to the landmark 1924 "Tournier Case" (*Tournier* vs. the *National Provincial* and *Union Bank of England*). Common law and guidelines resulted from that decision, and thus the case had become necessary background for management employees in the banking industry.

The Tournier Case concerned a bank customer with a £10 overdraft, who, having no fixed address, gave his bank branch manager the name and address of his new employers. When he defaulted on repayments, the branch manager telephoned those employers to ask if they knew his customer's address. In the course of doing so he disclosed the overdraft and default, and expressed his opinion that his customer was betting heavily. As a result, Tournier lost his job, sued the bank, and won his case upon appeal.

What came out of the decision was a set of four exceptions on the banker's contractual duty of confidentiality where customer information could be disclosed without their consent:

(a) Where disclosure is under compulsion by law;
(b) Where there is a duty to the public to disclose;
(c) Where the interests of the bank require disclosure;
(d) Where the disclosure is made by the express or implied consent of the customer.

Since the Tournier decision, banks have become extremely sensitive about protecting customer information. Strict privacy policies have been put in place, and systems containing personal information have been protected from unauthorized use and manipulation. Recent advances in security and encryption technology allowed banking customers to access their accounts and conduct simple transactions though online and telephone banking systems.

Employee Privacy in the Banking Industry

Employee privacy was somewhat different than customer privacy. By design, in most banks, customers were provided with the best level of privacy protection available. However, there were legitimate reasons why banks might want to monitor what employees were doing on company time and with company equipment.

For banks like CIBC, providing employees with access to company e-mail had become a strategic necessity. However, with e-mail access came the possibility of unwittingly receiving or transmitting an e-mail worm or virus, much like the ones which swept across the world in early 2000. (For an explanation of worms and viruses, see Exhibit 1.) Computer Economics Inc., a research firm based in Carlsbad, California, reported that the ILOVEYOU virus alone had infected three million computers around the world, causing US$2 billion in direct economic losses and a further US$6.7 billion in lost productivity. Insurer Lloyd's of London announced on May 8, 2000, that computer viruses would prove to be the biggest insurance risk in upcoming years, prompting business analysts to call for a widespread change in company e-mail policies.

In addition to protecting company systems from viruses, employers like CIBC had obligations to ensure that employees were not acting illegally, for example, in perpetrating frauds, or immorally. E-mail could be used by employees to make inappropriate or defamatory comments. It could also be used to transmit sensitive corporate information, without appropriate security.

CIBC's Electronic Communication Policy

E-mail and voice mail were both included in Section 4.6 of CIBC's *Principles of Business Conduct.* CIBC recognized that occasional personal use could not be avoided.

> E-mail and voice mail are essential ways to communicate with employees, customers, suppliers, and other parties. Although all e-mail and voice mail facilities supplied by CIBC are its property, CIBC recognizes that incidental or occasional personal use of both is unavoidable.

CIBC reserved the right to access and monitor both internal and external e-mail and voice mail, including stored messages, and to restrict the use of both, without prior notice. The company also reserved the right to produce all office communications in legal proceedings.

Assentor Software

To ensure that its brokerage employees were not acting inappropriately in their dealings with customers through e-mail communications, CIBC relied on software to screen and archive e-mail messages in a central database. The software had the ability not only to screen key words, but combinations of words and sentences (so called natural language technology). The software allowed CIBC to "flag" and hold potentially inappropriate e-mail communications, such as high-pressure sales tactics, insider information, as well as other potentially litigious issues, such as sexual harassment. These flagged e-mails were then held for human analysis and review before being sent.

The market for e-mail screening software was worth $17 million in 1999, and was growing at a rate of 45 percent per year. According to a report by the Tower Group (www.towergroup.com), natural language technology was a significant improvement in screening technology allowing for more flexible and accurate monitoring than keyword or phrase search alone.

An excerpt from a news release from SRA International Inc. (which markets Assentor e-mail screening software), dated Feb. 22, 1999, read:

> (Tower Group) predicts that natural language functionality will become the technology of choice for e-mail compliance tools. . . . Securities firms of all sizes are using Assentor to apply technology to the compliance review process and take advantage of the many benefits of e-mail technology for communicating with their clients. Assentor uses a sophisticated, linguistics-based natural language pattern matching engine and highly refined compliance patterns developed closely with securities industry associations, compliance experts, and major broker/dealers to ensure that the technology is effective for all types of compliance requirements.

Companies in the financial services industry which used Assentor included CIBC, A.G. Edwards, BancBoston, Southwest Securities, and the National Association of Securities Dealers. Many others used other, mostly less powerful, e-mail screening methods.

Call centers typically tape conversations for quality control, and most organizations announce to the customer at the beginning of the call that the conversation will be taped. Employees working at call centers knew when they arrived at work that their conversations would be taped due to the possibility of disputes—for example, replaying a taped call would confirm if the customer requested a "buy order" of 500 shares instead of a "sell order" for 5,000 shares of the same stock. It was much easier, on the other hand, to forget that e-mail use could be monitored.

CIBC had recently developed an "Electronic Mail Policy," which went into more detail than the previous entry in its *Principles of Business Conduct* document. This policy outlined appropriate and inappropriate use of this company resource. A short summary of the policy read:

> Electronic mail (e-mail) systems, provided by the CIBC Group of Companies (CIBC Group), are its property. Employees are to use these systems for company business primarily within the boundaries of this policy and its standards. Business information, and the ability to freely communicate it, are valuable assets that play a significant role in CIBC's success. The protection and appropriate use of these assets is everyone's responsibility.
>
> All messages sent or received by electronic mail are CIBC records and must be handled in a manner consistent with CIBC record management policies and practices. Caution and discretion should be used in the nature and content of all messages sent, stored or distributed.
>
> CIBC recognizes that incidental or occasional use of e-mail for personal communications is unavoidable. However, all users with access to CIBC e-mail systems should be aware that the CIBC reserves the right to access, to monitor and to archive all e-mail messages, transmitted, received or stored on its systems, without further prior notice.

"E-mail use is often similar to casual conversations rather than formal written communications," stated Jones, "because employees forget that it is recorded and can be monitored." Jones went on to stress that e-mail is a business resource covered by a separate e-mail policy. He concluded by asking, "How should employees be discouraged from inappropriate language, content and usage?"

Jones knew that these were not easy questions to answer. Recent articles in newspapers and trade journals on e-mail privacy, such as the following excerpt, had brought the issue to CIBC's attention once more.

"Prying Times: Those Bawdy E-Mails Were Good for a Laugh—Until the Ax Fell," *The Wall Street Journal,* Feb. 4, 2000.

In the course of their inquiry, workers say, managers found a number of potentially offensive e-mails, some of which had been sent by or forwarded to other employees in the office. That led to a wider investigation, and ended Nov. 30th 1999 when the Times fired 22 people in Norfolk, plus one in New York. Roughly 20 more workers, who the company determined had received offensive messages but didn't forward them to others, got warning letters. Most of the fired employees were otherwise in good standing; one had just received a promotion, and another had recently been commended as "employee of the quarter."

Some corporations, like CIBC, used e-mail screening to catch e-mail misuse, but since these filters tended to slow down network traffic, the practice was not universal. A second option, according to Jordan Worth, an Internet analyst with International Data Corporation, an Internet research firm, was to put in place policies that banned certain "types" of attachments. A third approach was to archive e-mail, but only access it in the event of a complaint.

EXHIBIT 1 Explanation of Worms and Virus

Viruses

A virus is a piece of programming code usually disguised as something else that causes some unexpected (and often undesirable) event, and which can automatically spread to other computer users. Viruses can be transmitted by diskette or CD, by sending them as attachments to an e-mail message or by downloading infected programming from the Internet. The source of the e-mail note, downloaded file, or diskette is often unaware of the virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are playful in intent and effect, while others can be harmful.

Generally, there are four main classes of viruses.

File Infectors

Some file infector viruses attach themselves to program files, usually selected COM or .EXE files. Some can infect any program for which execution is requested, including SYS, .OVL, .PRG, and .MNU files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programs or scripts sent as an attachment to an e-mail note.

System or Boot-Record Infectors

These viruses infect executable code found in certain system areas on a disk. They attach to the DOS boot sector on diskettes or the Master Boot Record on hard disks. A typical scenario is to receive a diskette from an innocent source that contains a boot disk virus.

Macro Viruses

Macro viruses are the most common form of viruses. Each macro virus can only be spread through a specific program. Most common types are Microsoft Word and Excel viruses. These programs contain "auto open macros" and "global macro templates." Virus writers recognize that any macros stored in the global file will automatically execute whenever something is opened. Macro viruses exploit these two aspects to enable themselves to replicate.

Worms

A worm is a special type of virus that transfers itself from one computer to another via a network. Worms can replicate themselves very quickly (often through e-mail address books) and thus carry the potential to overload host systems. Normally, worms cannot attach themselves to other programs, and thus do not pose a threat to files or data.

Source: Cases in Electronic Commerce, 2nd ed., by S. L. Huff, M. Wade, and S. Schneberger, McGraw Hill, 2002

Questions:

1. When was Canadian Imperial Bank of Commerce formed? What major products or services does Canadian Imperial Bank of Commerce provide through its electronic banking network? (10%)
2. Why does the use of email at work at Canadian Imperial Bank of Commerce become a hot topic of discussion in management circles? What alternatives does it take to deal with such hot issue? (10%)
3. What would you recommend to Canadian Imperial Bank of Commerce about the issues in customer privacy and employee privacy in the banking industry? (15%)
4. Develop a corporate code of ethics for Canadian Imperial Bank of Commerce according to the case described here and your knowledge about customer privacy and employee privacy issues. What should be the goal of this code? (15%)