Yahoo fired a loud shot back at Google by agreeing to buy Overture Services Inc. Yahoo agreed to pay $1.63 billion in cash and stock for Overture, months after buying another search-technology specialist, Inktomi, for $235 million. The moves will let Yahoo reduce its dependence on Google, currently the primary search engine for Yahoo searches.

Microsoft is also waking up to the power of Google and racing to protect its turf. The Yahoo deal has ripples for Microsoft, since the software giant has been a big Overture customer. But early this year Microsoft's MSN online group launched a project to develop its own search engine, with the goal of using search to increase MSN subscribers and advertisers. That could be a big threat to Google, given Microsoft's history of patiently eyeing new markets, then using its grip on PC software to dominate them.

Some industry executives think its technological lead is precarious, vulnerable to moves into its turf by the likes of Microsoft and Yahoo. Dominant market positions in technology tend to endure only if customers face a high cost of switching products, as with Microsoft's operating systems and Intel Corp.'s microprocessor chips.

Some rivals, particularly Yahoo, can blame themselves for helping Google take off. Three years ago. Yahoo picked Google's search engine to provide search results on Yahoo's network of Web sites, replacing a service by Inktomi. Yahoo had started by providing Internet searchers with information from its own directory, functioning like a giant Yellow Pages to the Internet organized largely by human editors. If this couldn't provide the information Yahoo would use Google's search technology. Increasingly, though, users went directly to Google's Web site for results.

As for Microsoft, it for years largely ignored Google and the search business. But search is also shaping up to be a central piece of Microsoft's next version of Windows, codenamed Longhorn. Longhorn is expected to enable PC users to search for information across all of their PC applications, such as Word and Outlook, as well as the Internet. A search engine built into Longhorn could pose a strong challenge to Google.

AOL Time Warner's America Online has also helped Google become big. AOL switched to Google's service for its U.S. customers 14 months ago. With Yahoo and Overture linking up, AOL may be more dependent on its relationship with Google.

Meanwhile, Google is starting to move onto the turf of online shopping companies. Late last year, it created a Web site called Froogle, which lets users search for books, apparel and virtually any other product for sale online.

Useful Terms and Definitions

E-commerce

The use of electronic transmission mediums to engage in the exchange, including buying

and selling, of products and services requiring transportation, either physically or digitally, from location to location.

Windows

Short for Microsoft Windows, a graphical user interface for DOS computers. Microsoft Windows provides a common way of using programs, making them easier to learn. Plus, Windows manages the way your PC works and takes care of common chores, such as working with the printer and disk drive. For example, when you set up a printer in Windows, that printer is automatically available in all your Windows programs. This lets us poor users concentrate on our work rather than on fussing with the computer and printer drivers or some such. Microsoft Windows provides access also to your computer's extended memory (memory above the first megabyte in your computer) and allows multitasking on 386 and higher computers

Lesson Two How the Internet Works

Key point: the terms and definitions of e-commerce

Difficult points: describing how Internet works

Requirements:

By the end of this lesson, you should be able to have a good command of

- useful terms given in the lesson
- preparing an English business card for yourself or for any other Chinese people

By the end of this lesson, you should be able to

- describe how Internet works
- give your idea about the business opportunity on Cellphones Ring

Abstract: The article introduces how the e-mail travels on the Internet, what a back bone provider is and how Internet companies connect to each other.

Key words: big carriers; online world; backbone provider; solution to safeguard competition on the Internet

To see how big carriers could control the online world, you must understand its structure.

How does E-mail travel on the Internet to reach someone far away?

When Jennifer, who lives in Pasadena, Calif, wants to send an E-mail message from her home computer to her mother in Washington, D.C., she uses a local Internet service provider (ISP) such as EarthLink Network Inc. (ELNK). EarthLink gives Jennifer access to the Internet, much in the way that an onramp puts a driver on the national high way system.

After Jennifer's computer makes a local telephone call to EarthLink's local bank of modems, Jennifer types in her E-mail message and hits "send". Based on Mom's E-mail address, EarthLink will recognize that Mom is a customer of an ISP in Washington called Erols Internet Inc. (RCNC). EarthLink will then send the E-mail to an Internet "backbone provider", such as GTE Corp. (GTE), to route it along its way.

What is a backbone provider and why is it important on the Internet?

Backbone providers are the Internet players that typically own and lease long-haul fiber-optic cables spanning a large region. They also own the communications gear that directs traffic over the Internet. There are only a handful of major backbone providers, including MCI, WorldCom, Sprint Corp. (FON), GTE, and PSINet Inc.(PSIX).

Backbone providers connect to each other to exchange data between their customers. They

also pick up and deliver traffic for a fee from the 7,000 or so smaller ISPs, who give residential and small-business users access to the Internet. Backbone carriers are like the highway system over which most of the freight of the Internet travels to reach its destination.

How did the current backbone providers come to be?

When the Internet was still a government-run system, there was only a single Internet backbone: the NSFNET, operated by the National Science Foundation, which connected the regional government-funded Internet networks that were run by various research universities. When the government privatized the NSFNET in 1995, companies such as MCI, UUNET Technologies (now owned by WorldCom), BBN (now owned by GTE), and PSINet stepped into the breach by setting up commercial Internet backbone services. Now, instead of one NSFNET backbone, there are many of them that link together to provide the global connectivity, that is the Internet.

How do Internet companies connect to each other?

When the NSFNET was privatized, the government set up three locations in the U.S. where various Internet backbone companies could place their communications gear side by side and connect to each other. These so-called"public peering points" are in Chicago. Palo Alto, Calif, and Pennsauken, N.J. Later, the government sanctioned two industry-run public peering points called Metropolitan Access Exchange East and West-MAE-East, in Vienna, Va., and Mae-West in San Jose, Calif.

The problem was, as the Internet grew, the public points became overburdened and traffic slowed at these bottlenecks. So backbone providers started making arrangements with each other, called "private peering". These are direct, bilateral connections between two carriers in which no fees are charged.

Do the Largest backbone providers charge each other?

Backbone providers aren't charging peers now, but there is a lot of discussion about whether they should. Most industry experts say the Internet needs to develop some payment scheme. After all, it is now a commercial, profit-making business, not a government freebie.

But the industry has not figured out how to calculate who owes what to whom. Without an industry standard or government regulation, smaller companies fear that larger ones will set these charges in an arbitrary and discriminatory fashion. There could be a lot of"cockamamie measurements," says Leonard Kleinrock, an Internet founder and computer science professor at the University of California at Los Angeles.

What is the solution to safeguarding competition on the Internet?

Since the Internet was privatized, it has grown by leaps and bounds into a remarkably successful communications medium without government regulation—and most want it to stay that way.

But the Internet has matured to a point that more uniform rules are needed to safeguard

competition. As a first step, experts argue that backbone providers should have to disclose the criteria for becoming a peer. This would allow companies to see whether they are being discerning a peer. This would allow companies to see whether they are being discriminated against.

An industry group called the Global Internet Project—whose members include such major backbone providers as MCI, GTE, and AT&T—is developing a longer-term solution. The group advocates a fair and public system under which all backbone providers would pay each other for carrying Net traffic.

"We need a market mechanism to ensure peering for all", says Daniel Schulman, president of AT&T WorldNet Service, a project member. Many issues need to be worked out, including who would do the policing. Still, with a clear payment system, those who can afford to pay the price can become peers. Peering would be determined by the market rather than by a private company with its own competitive interests.

New Words

carrier n.通信公司
online a.在线的；联机的；网上的
Internet service provider (ISP) n.因特网服务提供商
ramp n.斜坡；斜面；坡道
bank of modems n.调制调解器库
backbone provider n.主干网提供商
route v.按规定路径发送
haul n.传递或运输的路程、距离
communications gear n.通信控制装置，用来控制通信数据传输
destination n.目的地
NSFNET n.National Science Foundation Net 的缩写
breach n.突破口；缺口
privatized a.私有化的
public peering points n.公共对等汇接点，该点将几个主干网对等连接起来
sanction n.批准；认可
metropolitan Access Exchange n.城域访问交换点
freebie n.（美俚）免费品
arbitrary a.专横的；专断的
discriminatory a.区别对待的；歧视的
cockamamie a.（美俚）荒谬的；可笑的；令人难以置信的
by leaps and bounds 飞跃地；极其迅速地
criterion(pl) criteria n.（评判的）标准；尺度；准则
peer n./ v. 网络数语，指网络连接上的一种对等接入装置，也可用作动词，此处指可接入因特网的单位
discriminate v.区别；有差别地对待
advocate v.拥护；提倡
police v.管理；管制

Sentence Explanations

1. EarthLink gives Jennifer access to the Internet, much in the way that an onramp puts a driver on the national high way system. EarthLink（ELNK）为珍妮芙提供的因特网连通服务，就像提供一条通道把驾驶员送上国家高速公路系统那样。

2. They also own the communications gear that directs traffic over the Internet他们还拥有

指挥因特网信息传递的通信控制装置。 traffic over the Internet指因特网上数据信息的传送。

3. But the industry has not figured out how to calculate who owes what to whom但是，该行业还不知道如何计算谁欠谁多少。

4. Peering would be determined by the market rather than by a private company with its own competitive interests. 能否开展接入服务应该由市场决定，而不是由一个有着自己竞争利益的私人公司来决定。

Exercises（I）

1. Translate the following into English.

（1）FNET 被私有化后，政府在美国设立了三个地点，让各因特网主干网公司把他们的通信控制装置放在一起并互相连接。

（2）这些能量可以在生产过程中加以利用。

（3）问题解决之后我们都离开了实验室。

（4）他们的研究成果受到极大的重视。

（5）这块玻璃板在上星期做实验的时候就被打碎了。

（6）将这种器件很好地绝缘之后就可以把它安装在机器中了。

2. Please explain how e-mail travels on the Internet to reach someone far away.

Skill Training Business Card's Translation

一般公务名片包括：姓名、职务、单位名称、地址、电话等。下面分别看如何将它们翻译成英文。

1. 姓名

中国人姓名的英译应遵循汉语拼音的原则。即姓在前，名在后，按音译。须注意的是无论姓还是名，如果它的第二个音节以元音或以辅音 g, n 等开始，有可能与前面的音节发生连读时，可用连词符号"-"或隔音符号"'"把它们分开。如：王锡安，可译为：Wang Xi-an, 或 Wang Xi'an。姓名的前面可加头衔，如：Prof. ，Dr. 等，女性姓名前面视需要可加上 Miss，Ms.，Mrs.等。

2. 职务

职务的翻译主要靠借助词典，企业里的人员常常使用 manager。事业单位负责人，当你没找到更适合的词的时候，可用 director，如局长、部长、处长、院长、社长、所长、厂长、经理、董事、导演等。

3. 组织机构名称

组织机构名称的翻译应遵循两个原则：名从主人的原则和约定俗成的原则。名从主人指如果某单位已有自己的英文名称，我们不能擅自更改，只能尊重它原有名称。约定俗成指的是要符合英语国家的称谓习惯，不能按中文的意义生搬硬套。

组织机构的名称一般由四个部分组成：所在地区名、专名、类名和通名。例如：

Tianjin Hongda Science-technology Corporation 天津宏大科技公司

地区名 专名 类名 通名

其中，所在地区名和专名可用汉语拼音表示，类别名称和通名要按意译。并不是所有机构名称都必须由四个部分组成。有时可能由三部分甚至两个部分组成。如：Jiusan Society 九三学社。同样，有时专名也可以按意译。例如：Baoding Summer Palace Restaurant 保定颐和园餐馆。

如果是分支机构，有两种译法。一种是大机构在前，小机构在后。如：

China Pharmaceutical Co.,Tianjin Branch 中国医药公司天津分公司

另一种是分支机构在前，大机构在后。如：

Xiaohong Translation Service Centre, Tianjin Hongda Science-technology Co天津宏大科技公司晓虹翻译服务中心

4. 通讯地址

地址一般由专名和通名组成。通常专名按音译，通名按意译。地址由最小单位开始，由小往大按顺序翻译。注意，城市名称的后面不用通名。

例如：天津市河西区水上村高层 4 号楼 3 门 508 室

508 Ent 3 Tower 4 Shuishangcun Qtr. Hexi Dist. Tianjin

又如：北京市首都机场路丽都大楼 2 门 115 号

115 Ent 2 Lidu Bldg Capital Airport Rd Beijing

下面是一些常用的通名：

Province	省
Autonomous region	自治区
County	县
Township	乡
Town	镇
District (Dist)	（市辖）区
Quarter (Qtr.)	社区、住宅区
Estate (Est.)	社区、住宅区
Street (St.)	街、路（如果是：**东路，可译为：**St. East，依此类推。）
Avenue (Ave.)	大街
Road (Rd)	路、道
Alley	巷，里弄
Lane (La.)	巷，里弄
Building (Bldg.)	楼（普通大楼）
Mansion	（豪华型）大楼
Tower	塔楼，高层建筑
Villa	别墅
Entrance (Ent.)	门，入口（侧门：Side Ent.）

Flat (Flt.)	座
Floor (Fl.)	楼层
Room (Rm)	房间

名片常用的其他词汇如下：

Address (Add.)	地址
Post Code (P.C.)	邮政编码
Zip Code (Zip)	邮政编码
Post Office Box (P.O. Box)	邮政信箱
Fax	传真
Telex	电传
Telephone (Tel.)	电话
E-mail	电子信箱

下面看名片的实例：

Tianjin Telephone Equipment Factory

Wang Qian

Senior Engineer

145 Jianshan Rd
Tianjin,300053
China

Tel.(Ofc.) 02228286330
Fax: 02283319096
E-mail: wq@263.net

天津电话设备厂

王 前

高级工程师

中国天津市尖山路 145 号
邮编：300053

电话（单位）：02228286330
传真：02283319096
电子信箱：wq@263.net

Exercises（II）

1. Prepare an English business card for yourself.
2. Translate the following address into English.

a）北京市西城区复兴门外大街木樨南里 5 号楼 2 单元 803

b）天津市河西区马场道马场别墅 4 门 3 楼 306
c）天津市武清县杨村镇玉泉路 2 号
d）河北省保定市青年北路 258 号余门
e）中国天津市经济开发区第一大街 2 号

2. Translate the following organization into English.
a）太原九三科技开发公司
b）沈阳华联商厦
c）邮电部上海电话设备厂
d）中美合资奥迪斯电梯有限公司
e）天津市河东区大直沽街办事处

Reading Materials (A) Going Gold ?Maybe, if Enough Cellphones Ring

by Alee Foege

Abstract: According to IDC, cellphone users made 4.8 million purchases of ring tones in the United Stales in 2002. The phone will become some sort of media playback device.

Key words: cell-phone market; cell-phone users; ring tones

One of the most popular songs in the country last week,"Crazy in Love" by Beyonce Knowles, was not released only on compact disc and to radio stations. It was also sent to cell-phone users who wanted to download it as their ring tone. The music industry may be having trouble persuading people to buy its songs online rather than swap them without paying. But the cell-phone market is another matter.

Sometimes the ring tone is even more popular than the CD. Some 50 to 60 percent of all cellphones in the United States can download ring tones, according to Alex Slawsby, an analyst of mobile devices at IDC, a research firm. All major carriers offer the tones, and the market is expected to grow in part because virtually all new phones can receive them. Sometimes, an image of the artist appears on the phone as the music plays.

Cellphone users made 4.8 million purchases of ring tones in the United Stales in 2002, according to IDC, producing revenue of $16.6 million. The Yankee Group, another research firm, predicts that the revenue will be far higher this year, at about $50 million. Verizon Wireless, for instance, says 2.5 million of its customers are buying ring tones each month.

Some people in the music industry see a not-so-distant future when teenagers will pay a few dollars to download full songs onto their phones or other wireless devices."The phone will become some sort of media playback device".

Reading Materials (B) Radio ID Tags Spread Waves of Anger among Privacy Activists

by Simon London

Abstract: Radio ID Tags is the technology that solves a number of business problems—heft, counterfeiting, supply chain management. But without a concerted effort to address public concerns about privacy, RFID technology could face a public backlash.

Key words: Radio ID Tags; privacy; Privacy Activists

"Ultimately this technology will enslave humanity", says Kalhcrine Albrecht, a privacy campaigner and Harvard University doctoral student. The objects of her fire are radio-frequency identification (RFID) tags, slivers of silicon coming soon to supermarket shelves.

Gillette, the U.S. consumer products group, last month ordered 500m RFID tags for tracking packets' of razors through its supply chain. Michelin has developed a manufacturing process to vulcanize a tag into every lyre.

Sanjay Sanna, head of research at the Auto-ID Center at the Massachusetts Institute of Technology, says: "This is technology that solves a number of business problems—heft, counterfeiting, supply chain management".

But where companies see RFID lags as the 21st century successors lo barcodes, activists imagine a world where the movement of every object— and by implication every person— can be monitored.

Ms Albrecht, who runs Consumers Against Supermarket Privacy Invasion and Numbering, a group that opposes data collection by retailers, says many members "would rather walk naked than wear clothes that have been lagged".

Chris Hoofnagle, of the Electronic Privacy Information Center, a Washington- based watchdog says: "There are going to lie any number of entities who will want to use the information collected from RFID lags to track individuals or groups. The issue is control. Can you determine when the tag is active arid who is using the information collected"?

According to Caspian, proponents of the RFID tag envisage a pervasive global network of millions of receivers along the entire supply chain in airports, seaports, along roads, in distribution centers, warehouses, retail stores and homes.

This, Caspian says, would allow for continuous identification and tracking of physical items, enabling companies to determine the whereabouts of their products at all times.

An RFID tag consists of a silicon chip with a unique serial number. Pass the chip through a radio frequency Field and it can broadcast its identity for a few feet.

One of its big advantages over barcodes is that information can be collect-ed without a line of sight to the lag. This makes it possible to scan a pallet of goods simply by passing it through a radio field.

Moreover, RFID chips can store enough information to give each item, not merely each product line, a unique identity.

While the idea has been around for 30 years, the chips are only now becoming cheap enough for companies to consider widespread deployment.

Gillette is believed to be paying between 15 cents and 25 cents for each tag. Alien Technology, its California-based supplier, says the cost could fall to 5 cents or below if tags are made in high volume.

Procter & Gamble, the household goods group, is also running a pilot project. Retailers such as Wal-Mart, are also testing the technology, attracted by potential applications including "smart shelves" that sense when items are removed and re-order automatically, and checkouts that calculate totals when a shopping cart is wheeled through a radio field.

But it is possible to see how RFID technology could be misused and some consumers are taking steps to protect them-selves against being tracked. From a small office in Brooklyn, Stephen Galluccio sells bags lined with radio frequency-blocking material. "They are selling technology that does not turn off. You just don't have control any more".

Suggestions for an industry-wide solution range from Ms Albrecht's call for a total ban to self-regulation and restraint by companies.

Mark Roberti, editor of the RFID Journal, an online newsletter, argues for a code of practice that would switch off tags once they have been scanned at the point of sale, unless consumers agree for their purchases to be tracked.

The tag specification drawn up by the Auto-ID Center at the Massachusetts Institute of Technology includes a "self-destruct" command that would allow its owner to deactivate the tag.

Mr. Hoofnagle goes further. He calls on6 the government to set up a data protection commission to look at the privacy implications of RFID and other emerging technologies.

Epic has also called for the introduction of European-style data protection laws that control who can collect data and how it can be used.

On one thing, however, almost everyone agrees: without a concerted effort to address public concerns about privacy, RFID technology could face a public backlash.

"Privacy will become a huge issue for the RFID community as this technology rolls out", says Joe Tobolski at Accenture, the consulting firm.

Notes

RFID=radio-frequency identification 射频识别

by implication 含蓄地；暗示地

Useful Terms and Definitions

Defining Advertising

What is advertising? What are its important dimensions? The standard definition of advertising includes six elements. Advertising is a paid form of communication, although some forms of advertising, such as public service, use donated space and time. Not only is the message paid for, but also the sponsor is identified. In some cases the point of the message is simply to make consumers aware of the pro-duct or company, although most advertising tries to persuade or influence the consumer to do something. The message is conveyed through many different kinds of mass media reaching a large audience of potential consumers. Because advertising is a form of mass communication, it is also non- personal. A definition of advertising, then, would include all six of those features:

Advertising is paid nonpersonal communication from an identified sponsor using mass media to persuade or influence an audience.

In an ideal world every manufacturer would be able to talk one-on-one with every consumer about the product or service being offered for sale. Personal selling approaches that idea, but it is very expensive. Calls made by salespeople can cost well in excess of $ 150.

Marketers who have products and services for sale avoid the enormous expense of personal contact by using mass media to convey their messages. There the costs, for time in broadcast media and for space in print media, are spread over the tremendous number of people that these media reach. For example, $ 650,000 may sound like a lot of money for one ad on the Super Bowl, but when you consider that the advertisers are reaching over 100 million people, the cost is not extreme.

Word

（1）A collection of data bits that are processed as a unit. On the PC and with most microcomputers, a word is 2 bytes of data, 16 bits“wide”. Sometimes a word is as little as a byte (8 bits). The size varies, which is why we're being vague here. （2）A word processing program created by Microsoft (Word). （3）A unit of the English language, such as duh.

Lesson Three　A Crime Wave Festers in Cyberspace

Key point: useful sentences for establishing business relationship

Difficult points: Letter writing on establishing business relationship

Requirements:

By the end of this lesson, you should be able to have a good command of

- e-commerce terms given in the lesson
- useful sentences in letters of establishing business relationship

By the end of this lesson, you should be able to

- know the situation of the cybercrime
- tell of the ways to defeat snooping
- share your experience to against hackers

by Bob Tedeschi

Abstract: Cybercrime, long a painful side effect of the innovations of Internet technology, is reaching new dimensions. Spurred by a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing millions if not billions of dollars a year from businesses around the world, according to consultants who track cybercrime.

Key words: cybercrime; Internet technology; technically skilled thieves

Cybercrime, long a painful side effect of the innovations of Internet technology, is reaching new dimensions, security specialists say. Spurred by a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing millions if not billions of dollars a year from businesses around the world, according to consultants who track cybercrime.

Thieves are not just diverting dish from company bank accounts, these experts say. They are pilfering valuable information such as business development strategies, new product specifications or contract bidding plans and selling the data to competitors.

"Criminal activity on the Internet is growing–not steadily but exponentially, both in frequency and complexity," said Larry Ponemon, chairman of the Ponemon Institute, an

information management group and consultancy,"Criminals are getting smarter and figuring out ways to beat the system."

The number of successful, and verifiable, worldwide hacker incidents this month is likely to surpass 20, 000 above the previous monthly record of 16,000 in October, as counted by mi2g, a London-based computer security firm. Others have also offered dire estimates, although the dollar amounts are difficult to verify or compare because the definitions of loss vary so broadly. Part of the challenge in quantifying the problem is that businesses are often reluctant to report and publicly discuss electronic theft for fear of attracting other cyberattacks or, at the least, undermining the confidence of their customers, suppliers and investors or inviting the ridicule of their competitors. In one survey of 500 computer security practitioners conducted last year by the FBI and the Computer Security Institute, a trade group, 80 percent of those surveyed acknowledged financial losses resulting from computer breaches. The computer professionals took part in the survey on the condition they and their organizations would not be identified. Among the 223 respondents who quantified the damage, the aver-age loss was $2 million. Those who had suffered losses of proprietary company information said each incident had cost an aver-age of $6.5 million, while financial fraud averaged $4.6 million an incident.

One of the best-known cases of corporate computer crime involved two accountants at Cisco Systems, who after pleading guilty were each sentenced in late 2001 to 34 months in prison for breaking into parts of the company's computer system they were not authorized to enter and issuing themselves nearly $8 million in company stock.

But it is nearly impossible to identify the companies that have incurred the biggest losses, because of corporate reluctance to discuss what anonymous surveys have found to be a growing problem.

Computer security specialists who help protect these companies said the at-tacks were hitting major banks, telecommunications companies and other Fortune 500 companies and included a great variety of attacks."If people found out how astoundingly large this problem is, they'd be shocked," said James Hurley, an analyst with Aberdeen Group, a technology consulting firm. Hurley said one client, whom he declined to identify, suffered a $500 million case of electronic theft last year. Other consultants also recently recounted numerous examples of electronic thefts, but, like Hurley, they omitted company names because of confidentiality clauses in their contracts. Some examples, all provided by consultants who had seen the damage, include these: Last summer, someone hacked into the treasury system of a U. S. financial services company and transferred more than $ 1 million to what investigators presume to have been personal accounts. The company suspects it was an employee because of the inside knowledge required to gain access to the system. The investigation is continuing, but the employee's identity is still unknown.

In November 2001, a New York brokerage house noticed an intruder in its network from

overseas but did not know the nature of the intrusion. When a security form tracked him, they saw that he was re moving trading information on euros and using that data to compete with the firm while trading in markets in the Far East. The estimated damage was in the millions of dollars. Last spring, hackers broke into a U.S. $-based bank's database and gained access to accounts of wealthy customers. Millions of dollars was transferred overseas. The bank managed to undo most of the transfers, but total losses, including a security clean-up, were more than $1 million.

The weak economy is partly behind the rise in cybercrime, said Richard Power, global manager of security intelligence for Deloitte louche Tohmatsu, a business management consultancy. "In times of economic hardship, crime always increases", he said. "The more that money flows into cyberspace, the more criminal activity there'll be."

Corporations, meanwhile, are struggling to keep pace. With budgets and personnel stretched thin, companies that added many new technologies to their computer systems during the dot-corn build-up now find themselves lacking the resources to secure those systems against break-ins.

Part of the problem is that cybercrime is much harder to detect than crime in the physical world. "The vast, vast majority of virtual crimes right now never get caught or prosecuted, where you have some chance in the real world", said Dan Fanner, chief technology officer of Elemental Security, a computer security firm in Silicon Valley. "It is extraordinarily hand to prove anything using digital evidence."

Electronic crime is difficult to detect because it is so often an inside job. Security experts say the fastest-growing type of cybercrime involves theft of intellectual property—the pilfering of a company's plans for major projects, for instance, or marketing schedules and budgets stolen by an employee and sold to a competitor.

John Pescatorc, an analyst with Gartner Inc., a technology-consulting firm, estimated that in 70 percent of computer systems intrusions that resulted in a loss, an employee was the culprit.

In other industries, losses have become so widespread that accounting specialists are starting to call for fuller disclosure of cyberorimes by corporate victims, saying that customers and shareholders should know more about the losses and risks. Ponemon, the consultant, said companies often concealed the losses in their balance sheets. "It'll be recorded in different accounts that wouldn't have the same level of scrutiny as a loss", he said.

Such cover-ups do not allow for "a clean picture about how expensive it is to have to deal with fraudulent or criminal activities", Ponemon said. "This is becoming a very material part of the business model, so it deserves its own disclosure. That way, people can make better business; decisions whether to demand better controls or better technology or different precautions."

A securities lawyer cautioned against holding companies to a higher standard for disclosing cybersecurity breaches in all cases, lest they attract copycat attacks. "Sometimes it's more socially responsible a not to disclose, because it could multiply a company's losses by 20," he said.

But Jay Ehrenreich, senior manager of the cybercrime prevention and response group at Pricewaterhouse Coopers, said requiring broader disclosure of cybercrimes "makes a lot of sense and is something shareholders should demand". Still, he does not expect corporations to easily give in to such demands.

"A lot of times companies don't want to know what was taken," Ehrenreich said. "They just want us to find what the problem was and close the door, because there's a cost to finding out what was actually taken."

New Words

cyber- 前缀 有计算机或因特网的含义
cybercrime n.网络犯罪
spur v.刺激；鼓舞；鞭策
pilfer n.小偷小摸
figure out v.想出；弄清
practitioner n.开业者；实践者
anonymous a.匿名的
break into v.强行进入；闯入
victim n.受害者；牺牲者
scrutiny n.仔细检查；监视
cyberspace n.电脑空间；网络空间
cyberattack n.网络攻击
the rank-and-file n.普通老百姓；普通成员
exponentially ad.按指数地（增长）
FBI n.（美国）联邦调查局
fraud n.欺骗；诡计；假货；骗子
brokerage house n.经纪行
disclosure n.揭发；透露；被公开的秘密
shareholder n.股东

Sentence Explanations

Spurred by a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing mil-lions if not billions of dollars a year from businesses around the world, according to consultants who track cybercrime.

据追踪网络犯罪的咨询人员提供的信息，经济环境的恶化、网络空间上流动财富的日益增多，以及网络犯罪相对容易，造成每年数十亿，至少也有数百万美元从全球各个企业中被技术娴熟的窃贼和普通员工窃走。句子中 Spurred by…引起一个分词短语做状语，表示原因。

Exercises （I）

1. Tell of the ways to defeat snooping.
2. Share your experience to against hackers.（Read the following Reading Material first.）

Skill Training Business Letter Writing (I)

书信是电子商务活动中进行沟通的最主要手段之一。在本课和以下四课书中，我们将