HARVARD | BUSINESS | SCHOOL

9-308-015

REV: APRIL 22, 2008

F. WARREN MCFARLAN

ROBERT D. AUSTIN

JUNKO USUBA

MASAKO EGAWA

Secom: Managing Information Security in a Risky World

"There are serious issues with the measures taken to secure personal data". . . . Michinoku Bank became the first bank to violate the Personal Information Protection Law and receive warning from the Japanese government.

—*Nikkei Newspaper*, July 19, 2005

Mamoru Sekine, CEO of Jashopper, put aside a copy of an article of the *Nikkei Newspaper* and sighed. Several months had passed since the Personal Information Protection Law had come into effect in Japan. Yet information leaks of personal data continued, almost to the point of becoming daily press material. Just last month, Mastercard and Visa International had announced that the information of 40 million credit cards had been leaked due to a security breach of a contractor. It was not only small companies, like Sekine's, but major corporations with sophisticated technologies that were affected. As the CEO of an Internet business, Sekine had reasons to be concerned.

His eyes shifted to a proposal on top of his desk. The licenses for several cyber security services his company used were up for renewal. The cost of these services had little direct relationship with his company's hard-won profitability. Sekine had hoped that Jashopper might renegotiate better deals with IT vendors to maximize the funds invested in building profitability and reduce expenditures that did not obviously contribute to the return on investment. But the IT team had received service suggestions from Secom Trust Systems (Secom TS), a network integration and information security company, and together they cost more than the service Jashopper had been using. Of course the sensational newspaper stories made it clear that security was no place to economize. As he flipped through the product descriptions, Sekine wondered how he should go about choosing which products to use. Were the products worth the investment? How much protection was enough? Would his decisions change if his company decided to go public in a few years?

Professor F. Warren McFarlan, Professor Robert D. Austin, Research Associate Junko Usuba, and Executive Director Masako Egawa of the Japan Research Center of Harvard Business Schoool prepared this case. Research Associate Chisato Toyama assisted in the interviews. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

Jashopper.com

Jashopper, a small Internet company, hosted an electronic commerce site, Jashopper.com.[1] Retailers paid to place a virtual store on their site. Japanese consumers visited their site to purchase a wide range of products from electronic appliances to cosmetics and jewelry. In order to make a purchase, consumers had to register personal data such as name, address, date of birth, and credit card number. Sekine had started the company with a few friends three years ago. Their hard work had paid off; in the year just past, the company turned a profit for the first time. It now had annual sales of almost 1 billion yen (¥)[2] and 20 employees, as well as a set of established shops (400) and a strong base of consumers (600,000 registered). Sekine felt that the business was strong and was considering an initial public offering (IPO) to gain funds to grow the business.

Personal Information Protection Law

In 2006, Internet usage was commonplace in Japan with two out of every three people accessing the Web from computers or mobile phones (see **Exhibit 1**). Of Internet users, more than 36.2% had experience with Internet shopping.[3] But the increase in Internet usage had been accompanied by a rise in identity theft and elevated concern among the public (see **Exhibit 2**). In February 2004, Softbank BB, owner of Japan's largest Internet service provider, Yahoo! BB, announced the leak of 4.5 million users' data. Kakaku.com, a price-comparison website, lost 20,000 consumer data records to hackers. The city of Yuzawa, in northern Japan, inadvertently leaked the personal data of city residents while using file-exchange software (see **Exhibit 3**). Michinoku Bank lost CD-ROMs containing 1.3 million account holders including name, address, and account balance. Incidents resulted not from incursions by outsiders but from criminal acts of insiders (as at Softbank BB). Other incidents were caused by the careless actions of companies and employees (see **Exhibits 4a** and **4b**). These posed not only a threat to consumers but a significant financial burden to companies (see **Exhibit 5**). Softbank BB estimated the business impact to be ¥10 billion to ¥20 billion for compensation to customers, changing its security system and opportunity cost of lost business.[4]

In order to protect consumers from identity theft, the Japanese government enacted the Personal Information Protection Law in April 2004. This law applied to companies that managed databases with over 5,000 personal identities. Such companies were restricted from using personal information for purposes other than explicitly stated at the time the information was acquired. Further, they were required to take necessary measures to protect personal data from information leaks. In the case of an information leak, corporations and even individuals were punishable by law. The management and protection of personal identification information became a matter of compliance. Companies scrambled to meet the regulation by enforcing network security, setting up new company policies, hiring information security officers, and acquiring the Privacy Mark and ISMS Certification (see **Exhibit 6**).[5] Close to 1,600 organizations had acquired the Privacy Mark by mid-June of 2005.[6]

---

[1] Jashopper.com is a fictitious site.

[2] Foreign exchange rate was ¥117.29/$ as of March 31, 2007.

[3] Ministry of Internal Affairs and Communications, "2005 Report on Communication Usage Trend Survey," March 2006, p. 66.

[4] Isao Horikoshi, "Finally Started . . . the Realization that 'Net Users Are Basically Malignant,'" *Nikkei Communications*, May 24, 2004, p. 57.

[5] Privacy Mark is a certification issued by Japan Information Processing Development Corporation (JIPDEC), a quasi-government agency. It is issued to companies that meet certain standards for protecting consumer information and is valid for

Despite these efforts, security breaches continued even after the Personal Information Protection Law came into effect on April 1, 2005. Between April and June 2005 alone, 43 large-scale information loss or theft events occurred (see **Exhibit 7**).[7]

Other legislation added new challenges to managing and protecting information. A Japanese version of the U.S.'s Sarbanes-Oxley Law was being drafted by the government and expected to come into effect as early as 2008. The greater enforcement of internal controls would require better management of company information. The e-Document Law, which came into effect as of April 2005, allowed companies to keep documents required by the government electronically. Prior to the law's enactment, they were required to keep hard copies. For example, retailers could keep electronic copies of receipts that were less than ¥30,000 rather than having to physically store receipts. Such legislation created cost cutting opportunities but also raised the need for greater electronic storage and protection.[8]

Sekine thought about these challenges and their implications to his business. How would Secom TS's services help him meet these challenges?

The Secom Group

Secom[9]

Secom was the largest security service provider in Japan with a market share of over 60%. For the fiscal year ending March 31, 2007, the company had sales of ¥613.9 billion and operating profits of ¥97.8 billion.

The company started in 1962 when Makoto Iida, along with Juichi Toda, established the Japan Patrol Security Corporation, the first security service in Japan. The company offered patrolling services by security guards but initially struggled to gain customers as the concept of outsourcing security had not yet taken root in Japan. A break came in 1964 when it managed the security of the Tokyo Olympics. Thereafter, business grew steadily, but the company also suffered setbacks due to scandals involving theft by Secom's security guards. Iida focused on improving communication to and education of his employees but also realized the limitations to managing a large force of security guards, which were increasing as the business grew. In 1966, Secom introduced the "Security Patrol (SP) Alarm," a remote surveillance system that relied on sensors to catch intruders and fires. When the sensor detected irregularities, Secom would dispatch its staff to investigate the situation. Secom provided comprehensive security services by renting the sensors to customers, monitoring those sensors, and dispatching its staff in case of intrusion or fires. This business model was unique since,

---

two years. ISMS, also accredited by JIPDEC, is an ISO standard regarding comprehensive management and protection of information from policy setting and execution to continual revision of corporate security plans.

[6] Tsuneo Matsumoto, "Hitotsubashi ICS Management Law Class #12: Personal Information Protection Law and Privacy 2," *Weekly Toyo Keizai*, July 9, 2005, p. 106.

[7] Amount of loss or identity theft involving at least 1,000 customers' information. Yoshiya Katsumura, "Special Report: Why There Is No End to Information Leak," www.nikkeibp.co.jp/sj/special/09/, accessed August 14, 2006.

[8] Keidanren (Japan Federation of Economic Organizations) estimated the cost-cutting savings for e-documentation to be ¥300 billion for tax-related documents alone. "Sales Discussion of e-Document Law Begin—Proposing Data Usage Over Cost Cutting," *Nikkei Solution Business*, January 15, 2005, p. 50.

[9] The description of Secom is based on *My Biography* by Makoto Iida and interviews with Secom management.

in the U.S. or Europe, customers purchased their own sensors, and securities companies would monitor the sensors but did not dispatch their staff.

Even though customers lacked confidence in electronic surveillance and were slow to adapt, in 1970, Iida made the drastic move to switch his customers over from on-site security guards to SP Alarm. He lost 30% of his customers, but 70% converted to the electronic surveillance system. He also gained new customers, and the overall revenue increased. As the business expanded, the economies of scale worked to his advantage and improved the overall profitability of the business.

In 1974, the company listed on the Tokyo Stock Exchange and entered a phase of overseas expansion and diversification. In 1978, it established a joint venture in Taiwan and eventually expanded to the U.S., the U.K., Korea, Thailand, Malaysia, China, and other overseas markets. In the early 1980s, Secom expanded into new businesses such as new media. It established the Miyagi Network Corporation, a cable TV company, and participated in the establishment of the Daini Den-den, Inc. (the current KDDI, the second-largest telecom carrier in Japan) in the wake of telecommunication deregulation. It was around this time that Secom entered the information security business. It also entered medical services, insurance, and geographic information services.

As it diversified, the momentum of the security business was not lost. Secom introduced My Alarm, a surveillance and dispatch service for home, and Coco-Secom, a system for locating people, especially children and the elderly, through a global positioning system (GPS). As of March 2007, the company had contracts with 694,000 businesses offices and 390,000 homes. It had 2,100 emergency depots all over Japan. The security business was 70% of overall Secom Group sales and was responsible for most of the operating profit.

The Secom brand was well-known throughout Japan as the dominant security company. The logo was commonly seen on the streets of Tokyo, as Secom users liked to place the Secom sticker on their doors to ward off burglars (see **Exhibit 8**). The company had built a strong brand associated with security and safety through its security services and TV commercials, which featured national hero Shigeo Nagashima, a former baseball coach.

Secom Trust Systems

The start of Secom's information security business could be traced back to 1985 when it established Japan Computer Security with the newly privatized Nippon Telegraph and Telephone (NTT), which was the largest telecommunication company in Japan. Its main business was selling virus protection software to prevent contamination of floppy disks. That year, it also established two other network businesses: Video Techs Center (contents provider) and Secom Net (value-added network services).[10]

Secom started these businesses in hopes of leveraging the network knowledge it had gained through its core security business. Secom's remote surveillance system used an extensive computer network to collect data from sensors all over Japan to monitor homes and offices. By 1984, Secom was the owner of Japan's largest computer network, larger than that of any major corporation or information technology business. Through its operation, the company gained extensive knowledge in building, managing, and securing computer networks. In 1991, Secom Information Systems was established to manage Secom's vast network and to provide network system integration solutions to external clients. In 1994, it started a joint venture called Tokyo Internet that was an Internet service provider (ISP) for businesses. Eventually it would command the top position in leased lines. Through

[10] The value-added network (VAN) business involved the resale of private data communication lines.

this business, Secom gained experience with the Internet, helping customers access it. The business was sold in 1998. The same year, Secom entered the authentication market by leading the establishment of Entrust Japan Co. Ltd. with NTT Data, Sony Corp., Tokyo Mitsubishi Bank (the current Bank of Tokyo-Mitsubishi UFJ), and 13 other companies. In 1999, it officially kicked off its Internet security business and consolidated all of its related businesses to Secom Trust Net. In 2006, Secom Trust Systems Co., Ltd. was established through the merger of Secom Information Systems and Secom Trust Net to provide comprehensive information security and network system integration services.

Secom Trust System's Information Security Business

Secom TS offered a wide range of services including data centers, security audits, intruder detection services, digital certification, and consulting service (see **Exhibit 9**). In conjunction with its parent company, Secom, it had the advantage of offering a one-stop shop for both virtual and physical information security. It claimed to have no direct competitors that offered such a wide range of service; however, it had competitors in each segment, such as Verisign, the Japanese subsidiary of U.S.-based Verisign, the leader of the SSL certificate industry, in digital certification.[11] It served a wide range of customers from small to large companies, such as megabanks.[12]

One of the key features of Secom TS's information security was its Secure Data Center (SDC), claimed to have one of the highest standards of security in Japan and the world. At the center, both physical and cyber protection was provided 24 hours per day, 365 days per year. The physical protection was based on Secom's expertise in the security business over the last 40 years. The building was fortified by patrols, metal detectors, retinal scans, and cameras. The servers were housed in climate-controlled rooms, required due to the amount of heat given off by the servers, and the facility was backed up with power generators in case of power outage. The center was separated into seven security levels. The area with the highest level of security contained servers housed in special shelters to protect against electromagnetic waves, fire, and earthquakes. This center was originally built to house certificate authorities that issued digital certification and thus required extremely high levels of security. Over time, the physical size of servers had decreased relative to capacity, placing greater power demands per square feet of data center space. Secom TS had recently completed construction at the SDC to expand the overall power capacity.

The Product Decision for Jashopper

The license for several cyber security products and services used by Jashopper were up for renewal. Just a few days ago, Secom TS had brought in a product proposal for several information security products. Sekine took this proposal in his hand and started to flip through the pages and thought about the needs of his business (see **Exhibits 10** and **11**).

---

[11] Author's interview with Eiji Jinbe, head of Special Sales Second Division, Secom TS, August 9, 2006.

[12] Secom TS was entrusted with the management of certificate authorities for the Bank of Tokyo-Mitsubishi Bank UFJ and Mizuho Bank. This system was certified by Identrus, a banking certification system that is developed and adopted by major financial institutions in the world.

Hosting/Housing Service

A major decision had to be made on how the company was going to manage its servers. Currently, Jashopper used a small rental server company and was considering upgrading its servers in anticipation of expansion. The company had the option of buying its own servers and storing them on its own property or renting space at a data center (housing). It could also rent servers from a data center (hosting). Sekine's company needed approximately five servers for Internet functions and to host the Jashopper website. He believed that all this could fit into one-fourth of a rack space. Jashopper had six global IP addresses, which were needed for the company website and other communication devices.

Secom TS offered the following services through its SDC.

Server hosting Internet (DNS, mail, and Web) server hosting service was provided at the SDC. Secom TS provided the server, setup, Internet connection, and 24-hour help desk every day of the year. Security features were also included such as firewalls and monitoring for hackers 24 hours per day, 365 days per year based on Secom Intrusion Detection Service (IDS, described in greater detail in the next section) and SSL server certification. The initial setup cost was ¥250,000, and a monthly fee of ¥150,000 was required for basic services for one IP address. In addition, an Internet connection cost of ¥100,000 initially and ¥100,000 per month was required.

Advanced housing Secom TS provided racks to house customers' servers in the SDC. The customer was responsible for purchasing and setting up the server. Most of the security features offered in the IDS were included except for SSL server certification. Furthermore, Secom TS monitored to see if the server was working and alerted the customer if it stopped. The initial setup cost for one rack was ¥400,000 and ¥500,000 per month for up to eight IP address. Racks could also be rented out from one-fourth of a rack for an initial cost of ¥200,000 and ¥200,000 per month. Larger sizes were also available such as five racks for an initial cost of ¥1.6 million and a monthly fee of ¥2.1 million. The same Internet connection cost applied as that for the server hosting service. Although the customer was responsible for equipment, the advanced housing option did include climate control, multiple connections to the power grid (with backup diesel generators and uninterruptible power supplies (all redundant), redundant physical connections to the Internet backbone, and physical security (guards, strict access to equipment), all supplied by Secom TS.

Secom TS provided advanced housing to clients like Glaxo Smith Klein Japan, the Japanese arm of the major British pharmaceutical company. Such companies required a high level of security to protect information on clinical studies and consumer data. If large pharmas trusted Secom TS, surely it must have strong security measures in place. Sekine could also choose from many other data center operators ranging from small rental servers to large-scale carriers.

Monitoring and Protection Service

In addition to the data center, Secom TS offered a wide range of monitoring and protection services, including services to monitor the physical environment. If Jashopper chose to maintain its own server internally, it would need to buy firewalls and intrusion-detection software and hire staff to maintain them. On the other hand, in a data center, basic security functions could be included as part of the service. Basic security functions could also be enforced by purchasing additional features such as the Secom Intrusion Detection/Prevention Service.

Secom Firewall Service Secom TS provided both the hardware and software to enable firewalls preset to customer specifications. The company provided timely patches[13] and software upgrades and replaced firewall equipment in case of failure. The firewall was monitored 24 hour per day, 365 days per year, and the customer was contacted immediately when an issue with the firewall was detected. The initial setup cost was ¥80,000, and ¥40,000 was required per month for basic services to protect a company's gateway.

Secom Intrusion Detection Service[14] In general, an intrusion-detection system (IDS) was a security management system to monitor data lines and detect intruders into a network. An Internet detection system gathered and analyzed information flows (called "packets") to identify potential or actual security breaches and notified network administrators in event of a threat by phone and e-mail. In Secom TS's service, security experts remotely monitored the customer's network 24 hours per day, 365 days per year via hacker-detection sensors placed inside the network. Secom TS checked the packets that were entering and exiting a network against Secom TS's security policy and categorized threats into three levels. If the sensors found a high-risk intruder, Secom TS informed the customer immediately. Secom TS provided information and suggested countermeasures, but for the most part, it was up to the customer to resolve the issue. Therefore, customers needed IT staff that was knowledgeable about computer networks. Secom TS also provided daily, weekly, and monthly reports on activity that might indicate illegal access. There were two special features in Secom TS's IDS service. First, Secom TS conducted vulnerability assessment of the network and recommended countermeasures twice a year. Second, in the case of a security breach, damages to the computer and information network were covered by insurance from Secom's general insurance subsidiary. The cost was ¥200,000 for initial setup and ¥240,000 per month for a one-year contract with up to six IP addresses.

Secom Intrusion Detection/Prevention Service In general, an intrusion-prevention system (IPS) was a preemptive approach to network security to respond to intrusion quickly. It collected information like an IDS but went further to shut out an intruder based on rules established by a network administrator. In Secom TS's IPS, most of the functions of its IDS service were included. The key difference was that Secom TS stopped harmful packets and shut out intruders based on security policies customized specifically to the customer's needs. The policy was fine-tuned based on packet information collected from IPS sensors in the customer's network. Packets were unique to each company depending on the type of application and data used by the company. But there was also a danger of "false positives"; a general security policy might determine that packets that were actually safe and necessary to service a customer were unsafe, then stop the flow of information that was necessary for a company's normal operation. Thus, customization was important to ensure appropriate handling of packets and smooth operation. The response to intruders within the prevention service was faster than the response to the IDS, as Secom TS would act and prevent the damage from spreading. Furthermore, Secom TS monitored not only the packet flow to and from a company's network but also within the network. Overall, companies were able to increase their security level and detail without hiring additional staff. A unique feature of Secom TS's IPS service was the vulnerability assessment, which was done in greater detail and frequency than that of the IDS service. Audits were conducted every day, and if an issue was identified the software policy was upgraded as soon as possible. The audit was based on the e-Secom Assessment 365 Service (described in detail in the audit section). The installation fee was ¥1 million, and the monthly fee was ¥250,000

[13] A "patch" is a software upgrade intended to correct a recently discovered defect in already released software. Patches are important in security contexts because they frequently eliminate unanticipated security vulnerabilities. A "patch" covered a "hole" in security.

[14] Secom had over five years of experience and protected 1,000 servers with the Secom Intrusion Detection Service.

for up to six IP addresses. In addition, purchase of IPS hardware (¥1.98 million) and aftercare service (¥594,000 per year) was required.

Sekine thought that these products could help strengthen the information security level without increasing IT staff. He thought that the IDS and IPS products could be used to monitor the server that contained the sensitive information of his consumers such as credit card numbers. Or he could also choose to provide the IDS to each shop listed on Jashopper.com. Sekine knew of other players in the IDS and IPS market. LAC, a Japanese company that provided network security and system integration services, was the best-known in this field. It had a strong reputation but also commanded higher prices.

Identification and Access Control System

This service was based on a card that contained an IC chip (IC card) and was used as a personal identification card. The IC card, named ID ONE, could serve multiple applications such as tracking entry/exit logs of card holders and limiting access to buildings, rooms, PCs, and laptops. For example, a person who wished to enter a building or room needed to place his IC card by a reader located at the entrance. The reader would extract the information in the IC chip and verify that the card holder had access to the building. The cost for an entry/exit system was ¥1 million for one entrance plus ¥300,000 for system engineering. The price to set up one card was ¥6,000.

A different type of reader could also be attached to PCs so that a person would have to slide in his IC card to use the PC. The cost of such a system included a server cost (¥600,000), system engineering fee (¥300,000), and software license fee of ¥10,000 per PC.

Sekine also wondered to what extent he needed to control the physical flow of information in his office. Secom TS had originally approached the IT team through the general affairs manager who was working with Secom to install office security surveillance. Typically in a Japanese company, cyber security was managed by the IT department and the physical security by the general affairs department. Sekine wondered if the two departments needed to be working together on information security issues.

Digital Certification Service

Sekine examined the two digital certification services presented by Secom TS. He understood that securing his site with some type of digital encryption was critical to protecting the information exchange and transactions with both his shop and end consumers. Secom TS was the second-largest player in the digital certification market after Verisign Japan.

Secom Passport for Web This was an SSL server certification service. It verified to consumers that the website actually existed and was operated by a valid business. It also allowed user data and transactions to be secured by 128-bit encryption so another person surreptitiously monitoring the transaction could not see the content. Once a company had cleared Secom TS's audit policies, it received an authentication sticker that was installed in the server (see **Exhibit 13**). The price was ¥65,000 per certificate per year.

Secom Passport for Member This was a client certification service. Once a user was confirmed as a valid client, a client certification was downloaded to the user's PC. The website checked the client certification to make sure that the computer accessing the site was a valid user. This could prevent unauthorized users such as hackers from accessing a website with a stolen ID and password. The price for the standard course was ¥300,000 for the installation. For 500 certificates that

could be issued within a two-year period, the monthly fee was ¥110,000 per month. For 1,000 certificates the monthly fee was ¥140,000, for 5,000 certificates ¥650,000, and for 10,000 certificates ¥1.5 million.

On Jashopper.com, shop owners needed to access the main site to gain information on consumers who had made purchases so that the shop could send them merchandise. Shop owners and employees used an ID and password to log in. Sekine wondered if Secom Passport for Member might offer more security. He thought that he could issue one certificate for each store on his website. Sekine also thought it interesting that Secom TS's SSL certificate was very similar to the logo used by the parent company in the security business (see **Exhibit 13**). He recognized the logo because he had seen it often on buildings and homes on the streets of Tokyo. Sekine wondered if there really was a technological difference between Secom TS and its competitor and how he should go about deciding whether or not he needed the product.

Audit

Sekine believed that his company had taken appropriate steps in dealing with security issues. He had a small IT team, which reported directly to him. They had learned cyber security on the fly, reading IT magazines and gaining information from fellow entrepreneurs and security-product vendors. They believed that they had standard security measures in place. They had established a corporate security policy and guidelines and used reputable security products available in the market. However, with the recent outbreak of security breaches, he wondered if he needed to go back to the drawing board. Secom TS offered several security assessment services. He thought that these services might be a good starting point to stepping back and revisiting security overall.

Secom Total Security Assessment This service identified weaknesses in the network, system, and physical environment that could lead to security breaches. Secom TS conducted customer interviews, checked the actual office environment, and assessed the network. At the end of two weeks, Secom TS delivered an assessment report that identified security measures and priorities. The price was ¥500,000 for one location with eight IP address.

e-Secom Assessment 365 Service This service checked an e-commerce site every day to identify security weaknesses in the server and Web application. Over 10,000 items were screened each time against Secom TS's security policies. Examples of test items were vulnerability assessments of the host server and to attacks from worms and viruses. The version, patches, and settings of software and operating systems were checked for weaknesses. Mail settings were checked to see if there had been any illegal access. The firewall used in the network was also checked for issues. When the site was deemed safe, a safety sticker was posted on the Web (see **Exhibit 14**). If security concerns were identified, Secom TS informed the customer about the issue and suggested solutions through a website. The safety sticker was removed if the client did not fix the issue within 72 hours. The initial installation fee was ¥100,000, and the monthly fee was ¥480,000 for one domain and four IP addresses.

Other Services

Secom TS also provided services to improve overall security and to help companies respond to the e-Document Law.

Security consulting services Secom TS offered consulting services for overall security solutions. It helped companies identify security issues, set up security policies, and educate

employees about security issues through e-learning. It also supported customers in gaining the ISMS or Privacy Mark.

e-Document Solutions Secom TS provided a variety of electronic documentation services that met the requirements of the e-Document Law. The time-stamp service issued digital certifications of when and at what time an electronic document was created. The electronic signature service issued digital certifications of who created and signed off on an electronic document. Both time stamp and electronic signature were required under the e-Document Law. Secom TS was planning to introduce an electronic document archiving service in the near future.

Jashopper did not apply for the Privacy Mark because the process was time consuming and Sekine and his team did not think that there was a substantial business impact. But with rising consumer concerns, he thought that the mark might help reassure consumers that his site was safe. Acquiring the mark for his company would, of course, require a significant additional expenditure.

Secom Proposal

Secom proposed three alternatives for Jashopper. The first, least-expensive alternative was to use the advanced housing service; Secom would provide an all-in-one package including both physical and cyber security. It would improve the security of the EC site by minimizing the threat of viruses and hackers and providing a fault-tolerant environment with antiseismic structure and network redundancy. This alternative required the initial cost of ¥300,000 and a monthly fee of ¥300,000 (see **Exhibit 11**).

The second alternative was to add an identification and access-control system in addition to the advanced housing service. Secom's ID ONE card equipped with large memory chips could control access to entrances, networks, and PCs. An electronic lock named TR2 controlled access to entrances and kept records of all entrants. It shut out access by unauthorized individuals and deterred crime by employees. SmartOn, which controlled access to PCs, specified applications licensed to each individual and encrypted all the files. For 20 employees, the ID card would cost ¥120,000, TR2 (entrance access control system) ¥1.3 million, and SmartOn (PC access-control system) ¥1.1 million; all the cost would be incurred initially.

The third alternative was to add a service to assess the vulnerability of physical and cyber security. Using the Secom Total Security Assessment service, Jashopper could analyze its current security level from four viewpoints: (1) organization/system/policies, (2) physical security, (3) data access control, and (4) network security. It would clarify the risk tolerance of the company and identify priorities and cost for various security measures. This audit service cost ¥500,000 and required two weeks.

Conclusion

As Sekine put down the Secom TS proposal, his eye wandered back to the article in the *Nikkei Newspaper*. He surely did not want his company headlining the top stories with such a scandal. Especially with such a young company as his, the consequences could be devastating, quickly ending the entrepreneurial dreams that he had worked so hard to realize. How could he protect his customers when larger and more sophisticated companies with deep pockets had failed?

Recently, the company had focused on growth; Sekine suspected that security had not been emphasized enough. He remembered that they had created an emergency response manual in the early years, when they heard of a company's security breach in the news. The IT team had updated it every month, but he could not remember when he last saw it. How could he encourage his employees to keep information security on the top of their minds? Sekine had been looking to hire a chief technology officer, but he wondered if he should hire someone who could also serve as a chief information security officer. Sekine remembered that 70%–80% of information leak incidents were caused by insiders.[15] In addition to hiring a chief information security officer, should he be thinking about bigger steps, such as reorganization or changing the work flows, to improve security? Would more staff training be required? Should he take explicit steps to encourage whistle-blowing? On the other hand, would focus on information security slow his company's decision making?

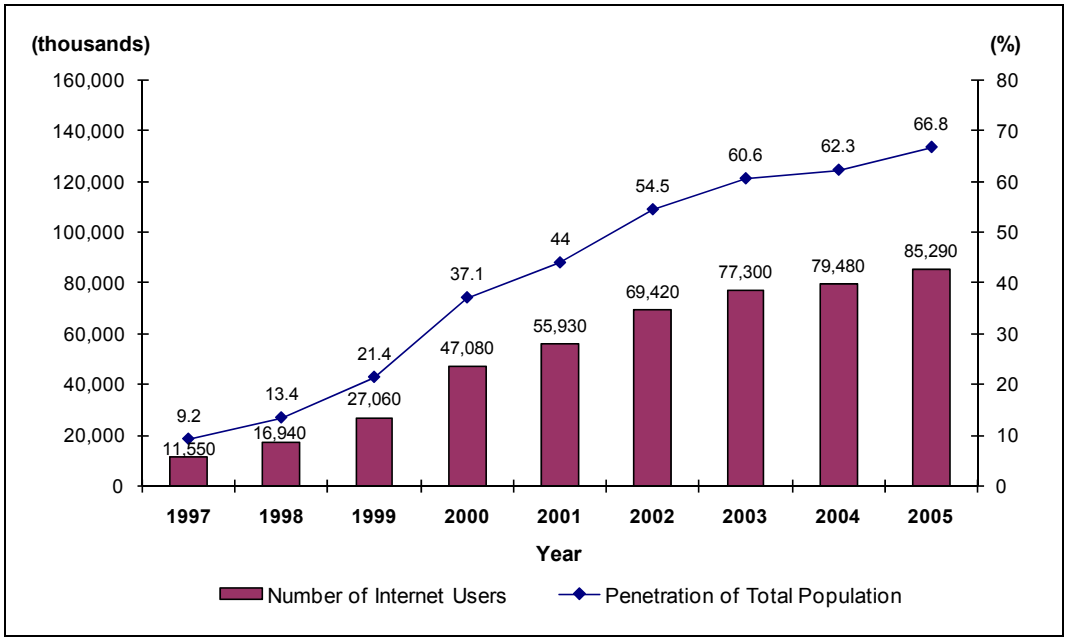
Sekine recalled his recent lunch with a friend from college who was a chief information officer of a large trading company. His friend indicated that the trading company invested significant amounts of money on information security without detailed analysis on investment returns, with the belief that information security was the backbone of a trading company and that the company should not take any risk on it. While information security was just as important for Sekine's company, he knew he did not have such resources. Then how much risk was acceptable for Sekine's fledgling venture?

Secom TS's representatives emphasized that Secom TS could act as a one-stop shop for all his company's information security requirements. Being able to outsource all related activities was attractive to Sekine, as Jashopper had limited resources. But he wondered which part of information security was critical to his core business; did managing internally make more sense for building the core competencies of his organization?

His eyes returned to the Secom TS proposal. Clearly, he could spend a great deal of money on security. And yet the Secom TS representative had been very professional in his acknowledgment that no amount of spending on security would *guarantee* that there would never be a security problem. The questions facing him could, at the highest level, be simply expressed: How much should he be willing to spend? How much security was enough?

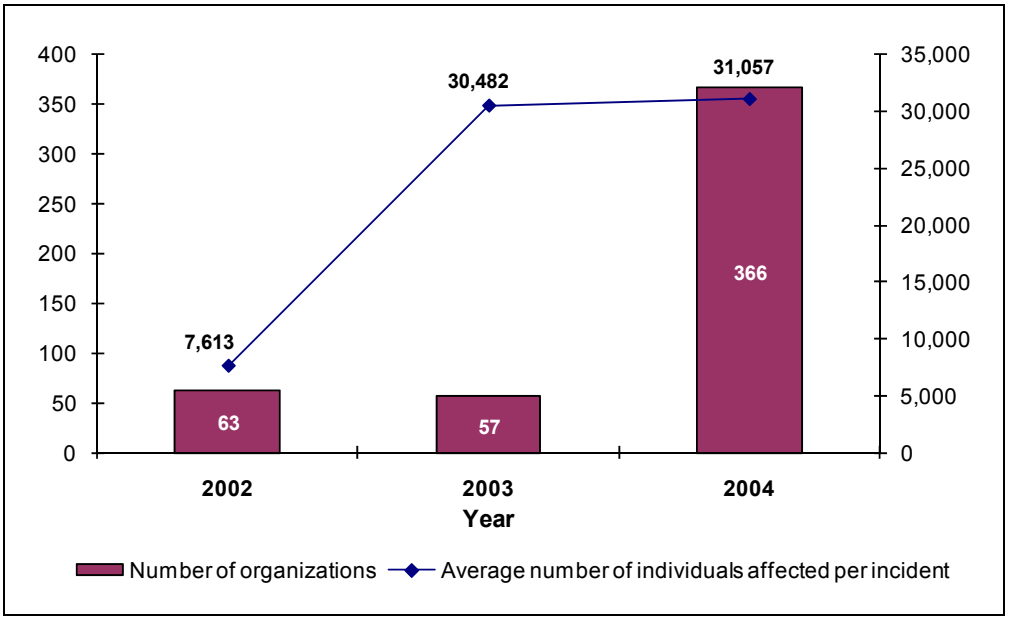
[15] Japan Network Security Association, "2004 Survey Report on Information Security Incidents (version 1.1)," January 10, 2006, p. 9.

Exhibit 1 Internet User Population and Penetration in Japan



Source: Compiled by casewriters using data from Ministry of Internal Affairs and Communications, "Communication Usage Trend Survey," March 2006.

Exhibit 2 Number of Information Leak Incidents and Individuals Affected



Source: Compiled by casewriters using data from Japan Network Security Association, "2004 Survey Report on Information Security Incidents (version 1.1)," January 10, 2006, p. 22.

Exhibit 3 Internet Security Terminology

Authentication Authentication is the process of determining if someone or something is actually who or what it declares to be. An example is the use of password and ID to log on to a computer.

Certification Authority (CA) A CA is an authority that issues digital certification.

Digital Certification A digital certification is an electronic data that establishes your credential in doing business over the Internet. It contains the digital signature of the credit authority that issued the certificate so that others can verify that the digital certificate is real.

File Exchange Software A file exchange software is a software used to share files among an indefinite number of computers on the Internet. Winny is the most well-known file exchange software in Japan.

Gateway A network point that is the entrance to another network, such as a company's intranet.

Internet Service Provider (ISP) An ISP is a company that provides Internet connection services to individuals and corporations, through its telecommunication lines and equipment. It also offers additional services such as e-mail and homepage hosting.

IP (Internet Protocol) Address An IP address is a 32-bit number that is used to identify the receiver or sender of information on the Internet or intranet. An address is given to communication equipment such as servers and client computers. A global IP address is given to equipment and computers that are accessed from outside a network from the Internet.

Phishing Phishing is a method used to steal personal identification on the Internet by posing as a legitimate entity on an e-mail or a website. The word is a combination of sophisticated, as the methodology used is quite sophisticated, and fishing.

Rack A rack is a shelf that is used to store servers that are often in the form of an electronic circuit board. A rack contains multiple slots to mount servers. The size is based on multiples of U, an international standard that is equivalent to approximately 4.5 cm.

Server A server is a computer that provides data and functions to other computers on the network. A Web server is a computer that contains the files and functions of a particular website. When another computer accesses a website, the Web server sends the relevant information over the Internet. A mail server is a computer that receives e-mail from other computers on its network and sends it out for delivery on to the Internet and sends e-mail on behalf of the other computers. A DNS server translates a domain name, which is similar to an address that identifies a computer network on the Internet, into an IP address.

Secure Sockets Layer (SSL) SSl is protocol that is used to encrypt data that is transmitted over the Internet. It is used commonly on websites to send personal information such as credit card numbers to prevent such data from being stolen by another party.

SSL server certification It is a service that provides digital certification of a website and SSL encryption. The website digital certification verifies that the site does exist and is operated by an organization that exists.

Spoofing Spoofing is when someone steals an ID and password and pretends to be an authorized user on the Internet. The imposter does illegal or bad activities and blames it on the authorized user.

Source: Compiled by casewriter based on e-words.jp and searchsecurity.techtarget.com.

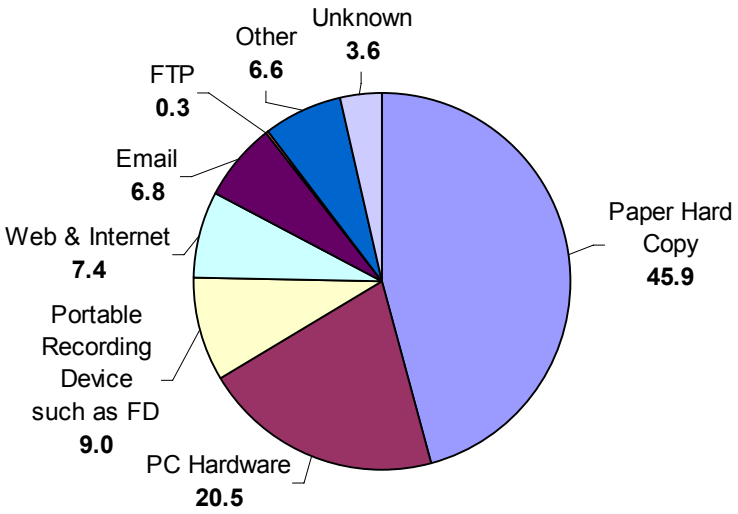
Exhibit 4a Causes of Personal Identification Leak

Technical Aspect	Cause	%	Examples
Nontechnical	Crime	46.7%	Information carried out against regulations, other crime by insider, data theft
Nontechnical	Human Error	24.3%	Lost, used information for something else
Technical Human	Error	22.1%	Failure in operation or setting up systems, mismanagement
Technical	Not enough measures taken	4.4%	Bug, security hole, virus, intrusion

Source: Compiled by casewriters using data from Japan Network Security Association, "2004 Survey Report on Information Security Incidents (version 1.1)," January 10, 2006, p. 25.

Note: This data is compiled from publicly available news sources.

Exhibit 4b Method Used for Personal Information Leak



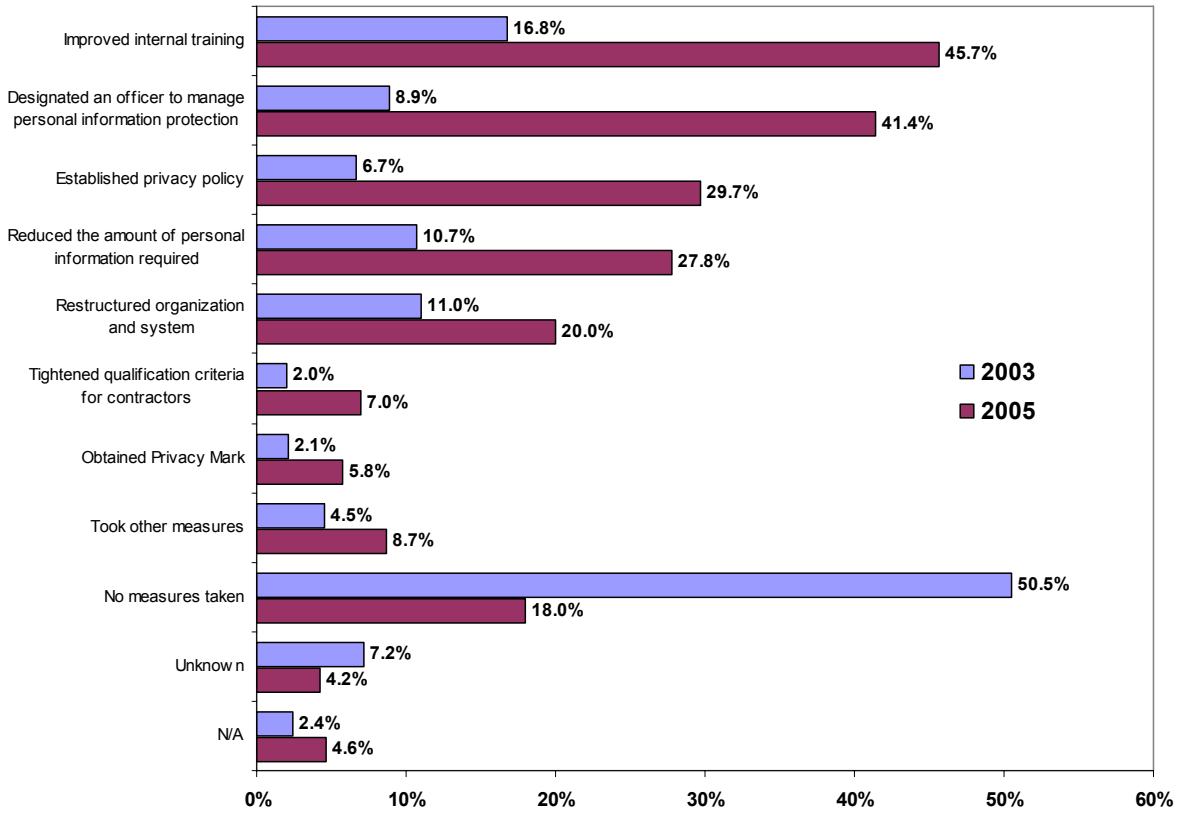
Source: Compiled by casewriters using data from Japan Network Security Association, "2004 Survey Report on Information Security Incidents (version 1.1)," January 10, 2006, p. 12.

Exhibit 5 Financial Impact of Information Leak Incidents

Organization	Incident and Timing	Impact on Business
Softbank BB (owner of Internet service provider Yahoo BB)	4.5 million users' information stolen by two insiders (February 2004)	Paid ¥500 to each user for compensation. Paid ¥4 billion to make systematic changes to prevent crimes. The next month of the incident new acquisitions dropped –36% compared to the previous month.
Kakaku.com (price-comparison site)	Website security was breached by SQL injection and 22,511 user e-mail address were stolen. Site users were redirected to another website that contained a virus (May 2005).	The website had to close down for 10 days. Lost sales and countermeasures cost ¥200 million.
Uji City Municipal Office (city government)	A part-time graduate student, sent from a contractor, stole 210,000 city residents' information using an MO (May 1999).	The courts ruled Uji City to pay victims ¥10,000 per person.

Source: *Nikkei Communications*, May 24, 2004, pp. 57, 60; *Nikkei Morning Paper*, April 10, 2004; *The Weekly Toyo Keizai*, August 20, 2007, pp.100–107.

Exhibit 6 Personal Information Protection Measures Taken by Companies



Source: Compiled by casewriters using data from Japan Network Security Association, "2004 Survey Report on Information Security Incidents (version 1.1)," January 10, 2006, p. 22.

Exhibit 7 Major Information Leak Incidents (April 1–June 30, 2005)

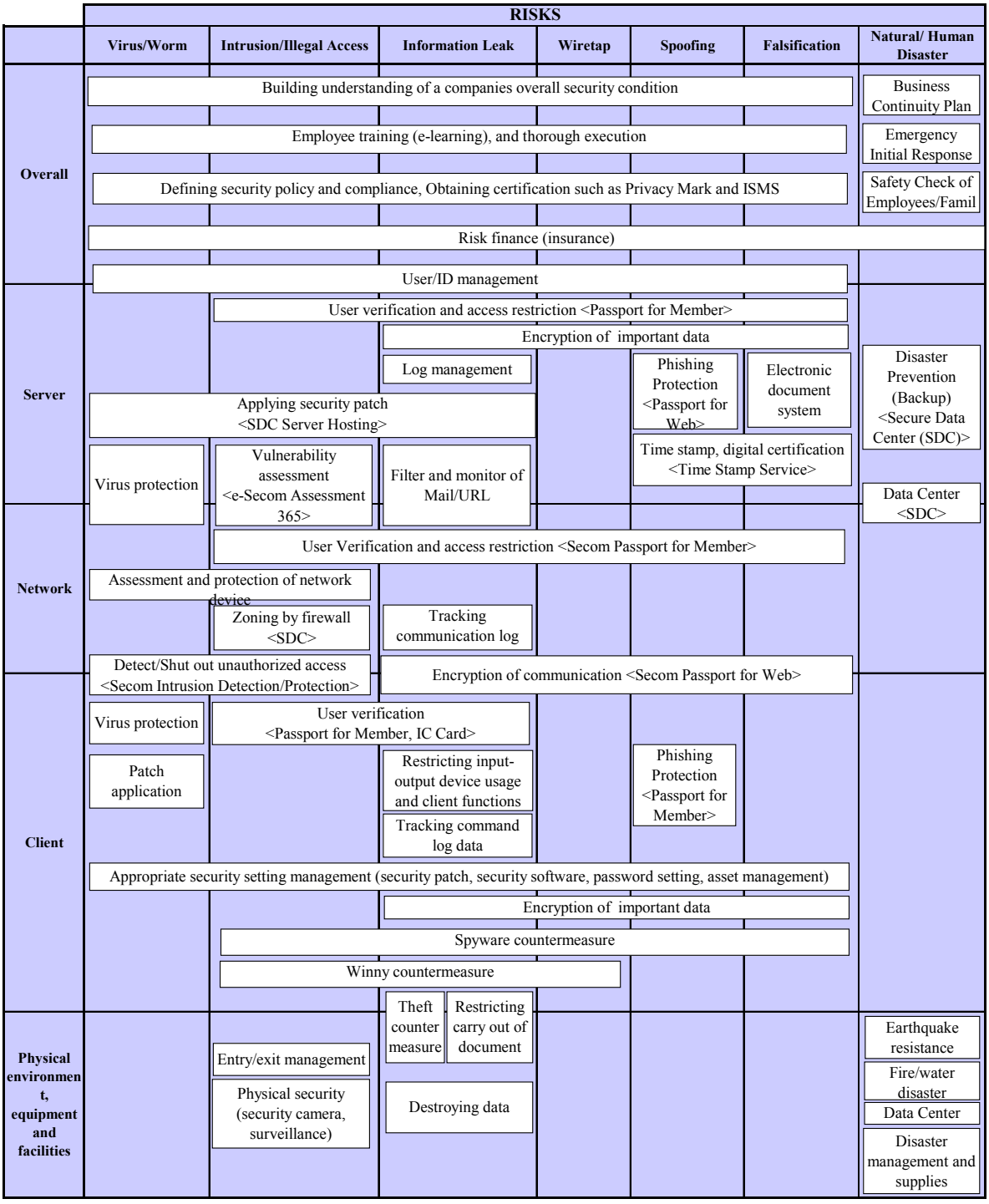
Date	Company	Incident
April 14	Yuzawa City	Leaked personal data of 11,255 residents by file shareware Winny
April 20	Michinoku Bank	Lost 3 CD-ROMs that contained 1.3 million bank customers' information
May 30	UBS Securities	Lost hard disk that contained 15,500 customers' information of UBS bank and UBS securities
June 1	Mitsubishi Trust Bank	Lost microfilm with 173,000 customers' information
June 14	NTT Communications	Laptop with 13,000 customers' information stolen from headquarters
June 18	All Nippon Airways	3 PCs with 5,300 customers' information stolen by subsidiary employee
June 21	Mitsubishi Electric	Lost USB memory containing 2,781 individuals who are part of national health insurance in a city in Kagoshima Prefecture
June 29	Adeco	61,876 personal data of registered temporary staff stolen by hacker from website
June 30	Mitsui Sumitomo Bank	Loses microfilm containing 61,405 customers' data
June 30	Kansai Urban Bank	Loses microfilm containing 52,000 customers' data
June 30	Risona Group	Loses microfilm containing 287,000 customers' data
June 30	UFJ Trust Bank	Loses microfilm containing 116,000 customes' data
June 30	NTT Docomo	Loses hard disk containing 48,000 customers' data

Source: Compiled by casewriters using data from Yoshiya Katsumura, "Special Report: Why There Is No End to Information Leak," www.nikkeibp.co.jp/sj/special/09/, accessed August 14, 2006.

Exhibit 8 Secom Home and Building Security Logo

Source: Secom, www.secom.co.jp/service/architectual.html, accessed August 16, 2006.

Exhibit 9 Secom Trust Systems Total Security Solutions



Source: Secom Trust Systems sales brochure. (Copyright 2006 SECOM Trust Systems Co., Ltd. All rights reserved.)

Note: This is a list of the different areas for which Secom TS provided solutions. Examples of specific services are listed in brackets <>.

Exhibit 10 Summary of Secom Trust Systems' Services

CATEGORY	SERVICE	DESCRIPTION		FEES		
				Initial Cost	Monthly Fee	Annual Fee
Hosting/Housing Service	Internet Connection (10M)	Mandatory for all customers		100,000	100,000	
	Server Hosting	Includes firewall, monitoring of 24/365 (IDS)	250,000		150,000	
	Advanced Housing		Per rack (up to 8 IP addresses)	400,000	500,000	
	Per		1/2rack	300,000	300,000	
	Per		1/4rack	200,000	200,000	
Monitoring/Protection Service	Secom Firewall Service			80,000	40,000	
	Secom Intrusion Detection Service (IDS)			200,000	240,000	
	Secom Intrusion Prevention Service (IPS)	Includes IDS and incorporates preventive approach	Up to 6 IP addresses	1,000,000	250,000	
	IPS		hardware cost	1,980,000		
	Afterca		re service		49,500	
Identification and Access Control System	ID ONE	ID card to be used for access control for entrance and PCs	Setup per one card (with R/W)	6,000		
	TR2	Entrance access control system	Per one entrance system (min. component)	1,000,000		
	Syste		m engineering	300,000		
	SmartOn	PC access control system	Per PC (software)	10,000		
	Serve		r	600,000		
	Syste		m engineering	300,000		
Digital Certification Service	Secom Passport for Web		Per certificate			65,000
	Secom Passport for Member		Standard course	300,000		
			500 certificates (within 2 years)		110,000	
Audit	Secom Total Security Assessment		Per location with 8 IP addresses	500,000		
Other Services	Security Consulting Service					
	e-Document Solutions					

Source: Company documents.

Exhibit 11 Estimated Cost for Jashopper

	Service	Description		Initial Cost	Monthly Fee
A	Advanced Housing	Internet Connection (mandatory)	Mandatory	100,000	100,000
		Advanced Housing	Per 1/4 rack	200,000	200,000
		Total		300,000	300,000
B	Identification and Access Control System (ID ONE, TR2 and SmartOne)	ID card (Y6,000 per employee)	20 employees	120,000	
		Entrance access control One	entrance	1,000,000	
			System engineering	300,000	
		PC access control	20 PCs (software)	200,000	
			Server	600,000	
			System engineering	300,000	
		Total		2,520,000	
C	Audit (Secom Total Security Assessment)	Analysis of the current security level	Per location with 8 IP addresses	500,000	

		Initial Cost	Monthly Fee
Alternative 1	A	300,000	300,000
Alternative 2	A	300,000	300,000
	B	2,520,000	
	Total	2,820,000	300,000
Alternative 3	A	300,000	300,000
	B	2,520,000	
	C	500,000	
	Total	3,320,000	300,000

Source: Company documents.

Exhibit 12 Information Stored on Jashopper's Computers

Customer Information

Customer name, billing and delivery address(es), telephone number, e-mail, and date of birth

Credit card number and expiry date

Records of past purchases and preferences

Customer customizable features (wish lists, etc.)

Shop Information

Shop description (address, telephone number, e-mail address, and owner's name, bank and payment transfer information)

Product information (description and price)

Delivery options

Payment options

Corporate Information

Development software (source code), version control system, testing systems

Production software (executable code)

Financial information

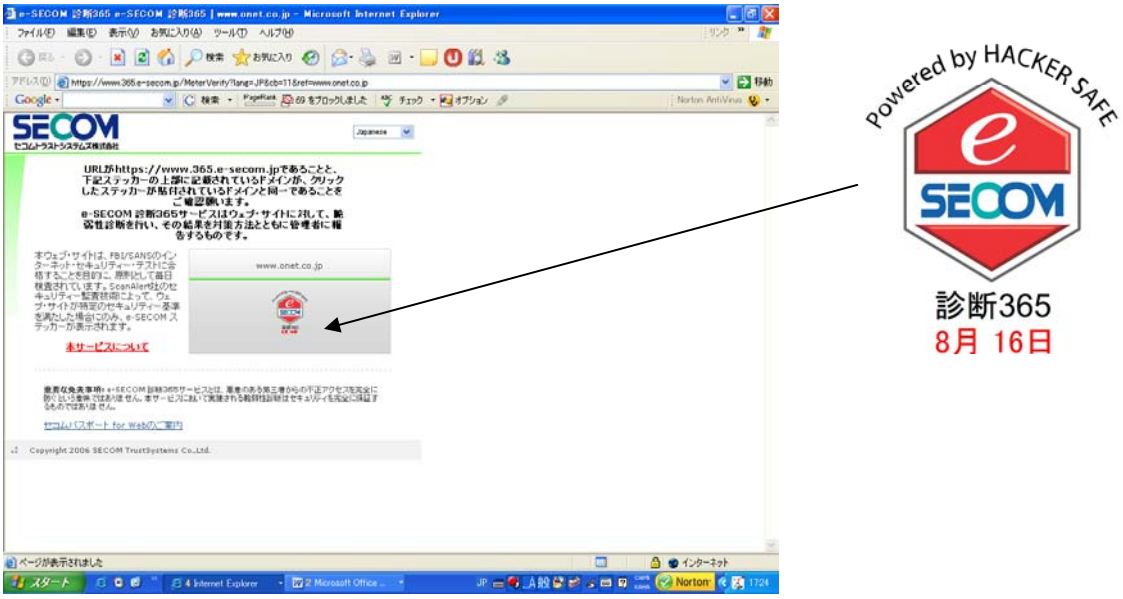
Personnel information (employee's name, address, telephone number, date of birth, social security arrangements, salary and bonus, performance evaluation and promotion records)

Source: Casewriters.

Exhibit 13 Passport for Web Certification

Source: Biccamera Inc., www.biccamera.com, accessed August 16, 2006.

Exhibit 14 e-SECOM 365 Assessment Service Logo and Website Verification



Source: OMMG Inc., www.onet.co.jp/cnt00/chance/indexcf.html, accessed August 16, 2006.