Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Computing and Information Systems

School of Computing and Information Systems

9-1999

Xcert Software, Inc.

Keng SIAU
Singapore Management University, klsiau@smu.edu.sg

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

Part of the Databases and Information Systems Commons, and the Software Engineering Commons

Citation

SIAU, Keng. Xcert Software, Inc.. (1999). *Journal of Information Technology*. 14, (3), 235-242.
Available at: https://ink.library.smu.edu.sg/sis_research/9396

This Journal Article is brought to you for free and open access by the School of Computing and Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Computing and Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

Journal of Information Technology (1999) **14**, 235–242

Xcert Software, Inc.

KENG SIAU

Department of Management, College of Business Administration, University of Nebraska-Lincoln, Lincoln, NE 68588-0491, USA

Xcert's business is in developing Internet and Intranet security enhancement technology. Xcert was founded in April 1996 by Andrew Csinger and Pat Richard and was headquartered in Vancouver, Canada. Xcert's solution to Internet security was a public key infrastructure (PKI). PKI is a system of digital certificates, certificate authorities (CAs) and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. Xcert's PKI technology allows organizations of any size to issue digital certificates to their members. These organizations become their own CA and are empowered to issue digital certificates to their individual client base. This case study is about a start-up company that is in transition from a dream stage to a reality stage. One of the issues that surfaces in the case study is intraindustry competition. Despite being an early entrant into the Internet security business, Xcert faced brutal competition from companies such as Entrust, Nortel, VeriSign and Netscape. The problems facing the company include (1) finances, (2) future direction and leadership, (3) structure, experience and size and (4) marketing. This is a very rich case study with a number of interrelated issues. The case serves two teaching aims. Firstly, this case allows students to confront and discuss real-life issues facing a start-up information technology (IT) company. The students analysing the case are asked to provide alternatives and solutions to the problems by putting themselves in the positions of the founders of the company. Students should come to understand the difficulty in managing a start-up company and the various trade-offs the management needs to make. Secondly, the case study introduces various Internet security concepts to students.

News Release – Software Sentry Technology Announcement

Vancouver BC (18 April 1996) – Xcert Software Inc.

A Vancouver-based software company has won the race to hit international markets with technology, announced today, that will provide organizations with a method to secure and authenticate business transactions on the Internet.

The Sentry Certificate Authority, also known as Sentry CA, is the final piece of a complex jigsaw that will make split-second electronic transactions as safe as traditional paper-based business deals. It is expected to unleash a tidal wave of electronic transactions – billions of dollars daily in business held back so far by corporate mistrust of the Internet as a hacker-prone battle zone.

Already, several major corporations are interested in using the Sentry CA developed in Vancouver by Xcert Software Inc. The breakthrough product, launched on the Internet today (http://x.509.com), is available to anyone for a 5-day free trial. Xcert is negotiating with potential technology and marketing partners to market the product.

Dr. Andrew Csinger, Xcert president and a computer science researcher at the Simon Fraser University, said 'We have taken the best of existing technology – the results of research from many different commercial and academic labs – and found a unique way of bolting it all together with our own software. We believe we are the first ones anywhere to have created a commercially-viable, workable product of this sort.'

Until now the Internet security market has been dominated by major players offering very expensive custom solutions for large corporate clients. The Sentry CA is an off-the-shelf solution aimed at everyone: virtual private networks, intranets, virtual communities or *ad hoc* collections of Internet users.

Among other uses, the Sentry CA will:

- Create electronic or 'digital' certificates that could be as legally binding as traditional signatures on paper.
- Integrate seamlessly with existing Internet products such as Internet browsers and webservers.
- Allow corporations (or any group) to take charge of their own security by allowing them to decide who receives a digital certificate.

0268–3962 © 1999 The Association for Information Technology Trust

- Allow access control based on these digital certificates (for instance to block out pornographic web sites from children, publish staff-only Internet sites, facilitate pay-per-view websites).
- Enable automatic billing over the Internet and Intranets.
- Build a profile of customer demographics and preferences (powerful tools in the advertising world.)

Introduction

Mission: Xcert's objective is to be the leading provider of products and professional services that enable its customers to become their own digital certificate authorities.

In April 1997, the founders of Xcert Software, Inc. were pondering the future of the company. Xcert won the race to produce an off-the-shelf Internet security product, Sentry CA, in 1996. In addition, Sentry CA was selected by *Network Computing* magazine as a nominee for its 1997 Well-Connected Award in the category of 'Enterprise Security: Best Key Management System'. In spite of these early victories, Xcert was facing difficulties a year after it was founded.

Although Xcert was an early entrant into the Internet/Intranet security business, it faced severe intra-industry competition. Its competitors included companies such as Entrust, Nortel, VeriSign and Netscope. In addition to external pressures from competitors, Xcert was facing internal pressures such as (1) finances, (2) future direction and leadership, (3) structure, experience and size, and (4) marketing.

Company background

Xcert's business was in developing Internet and Intranet security enhancement technology. It was founded by Andrew Csinger and Pat Richard in April 1996 and was headquartered in Vancouver, Canada.

The co-founder and president of Xcert, Andrew Csinger, worked as a consultant for several large corporations during the 1980s. He received a PhD degree in computer science from the University of British Columbia, Canada. He had done work in user modelling, artificial intelligence, GUI (graphical user interface) design and computer graphics. Pat Richard, the other co-founder and vice-president of technology and strategic planning, pioneered the integration of public key cryptography with directory technologies on the Internet. Pat developed the first World Wide Web (WWW)-based certificate authority (CA) and created the first public web site to use client authentication using digital certificates. Prior to founding Xcert, he had worked on distributed messaging technologies at Northern Telecom and Microsoft.

The two founders came together as a result of working for an Internet service provider (ISP). Andrew recalled:

> It turns out that Pat was well on his way towards his first prototype implementation of something very close to what I was looking for. I convinced him that there was a business here and that he did not have to give away his prototype to the Internet community, that he could sell it and make some money and still advance the democratization of the Internet.

The company had 18 employees as of July 1997 (as shown in Figure 1). Most of Xcert's employees were young and highly skilled in information technology (IT). Their skill placed them in great demand in an industry with a shortage of skilled computer professionals. The office environment was informal with employees spending long hours at their desks (or in front of the computers) and coming in to work at various hours of the day. Despite working in one of the prime financial districts in Canada, the employees dressed very casually – in T-shirts and shorts during the summer. Xcert operated like a typical research and development (R&D) environment but in the heart of a financial centre.

The Internet and electronic commerce

The Internet has grown explosively in the last few years. The number of people tapping into it has been doubling almost every 12 months. Electronic commerce is also growing on the Internet. The revenue generated from electronic commerce is expected to increase exponentially in the next few years. A recent study by International Data Corporation (IDC) indicated that the amount of revenues collected from Internet sales would increase 'dramatically' from $2.6 billion in 1996 to more than $220 billion during 2001. IDC reported that 'already one-half of electronic transactions are completed over the Web – as opposed to fax and phone. That number will increase to four-fifths by 2001.'

The main advantage of the Internet is that anyone with a computer and a modem can get on the Internet easily. This, however, is also one of its main drawbacks. Dishonest people can steal valuable information such as credit card numbers, phone numbers, addresses and other information when commercial transactions are carried out over the Internet. At the back of the mind of many organizations contemplating electronic commerce is the question 'How secure are Internet transactions?' For electronic commerce to take off in cyberspace, this major stumbling block, Internet security, needs to be resolved. The Internet security

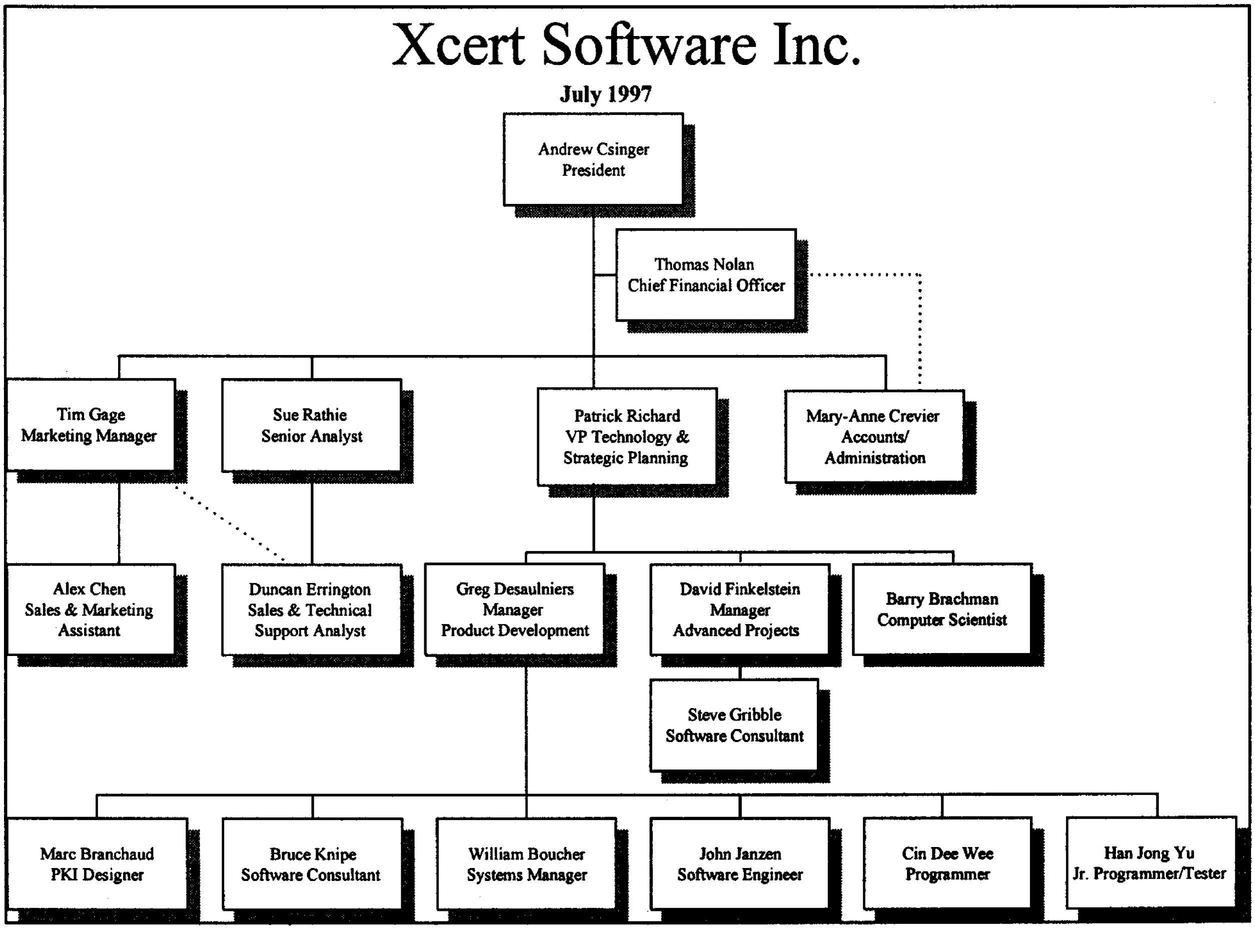
Xcert Software Inc.
July 1997
Andrew Csinger President
Thomas Nolan Chief Financial Officer
Tim Gage Marketing Manager
Sue Rathie Senior Analyst
Patrick Richard VP Technology & Strategic Planning
Mary-Anne Crevier Accounts/ Administration
Alex Chen Sales & Marketing Assistant
Duncan Errington Sales & Technical Support Analyst
Greg Desaulniers Manager Product Development
David Finkelstein Manager Advanced Projects
Barry Brachman Computer Scientist
Steve Gribble Software Consultant
Marc Branchaud PKI Designer
Bruce Knipe Software Consultant
William Boucher Systems Manager
John Janzen Software Engineer
Cin Dee Wee Programmer
Han Jong Yu Jr. Programmer/Tester

Figure 1 Xcert's organization chart

issue is the focus of intense research and experimentation. Most of the existing Internet security solutions involve digital certificates.

Digital certificates

Digital certificates (also known as public key certificates or security certificates) are a way of verifying someone's (or some company's) identity in the cyberspace. A digital certificate is the digital equivalent of a driver's licence, a credit card or an employee badge. The digital certificate contains information about whom it belongs to, who issued it, a unique serial number or other unique identification, valid dates and an encrypted 'fingerprint' that can be used to verify the contents of the certificate.

Existing approaches rely on some sort of central CA to issue and validate digital certificates. A CA is an administrative agency that verifies the identity of entities and issues digital certificates attesting to that identity (see Figures 2 and 3). An individual or entity wishing to send an encrypted message will need to apply for a digital certificate from a CA.

One problem with the use of a central CA is that the security needs of a bank are very different from those of a neighbourhood bookstore or a video game arcade. For a single digital certificate to be useful in such a wide range of contexts, it would need to contain or index a great deal of personal information about individuals and organizations – some of it highly sensitive. According to Pat

> There is no widespread, well-understood means of certifying individuals on the Internet today. Certifying a large number of individuals using the same mechanism that currently certifies web servers has not proven practical.

Public key infrastructure

Xcert's Internet security solution is based on a public key infrastructure (PKI). A PKI is a system of digital certificates, CAs and other registration authorities that verify and authenticate the validity of each party

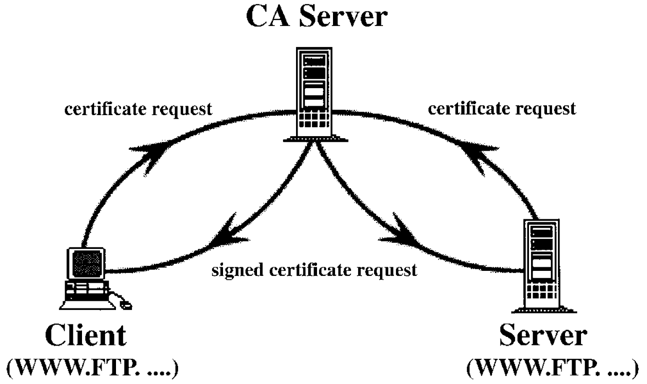

Figure 2 Certificate Authority (CA)

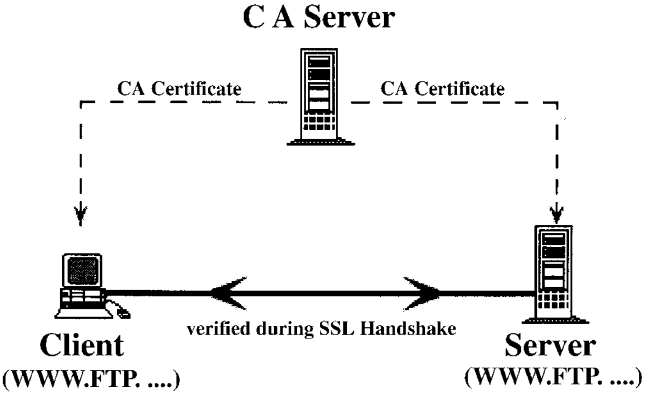

Figure 3 Server and client authentication

involved in an Internet transaction. It aims at managing and administering a public key system across the Internet. Two keys are used in a PKI, one known as the public key and the other is the private key. Data encrypted with the public key can only be decrypted using the private key. The owner of the key pair will release to the public one half of the key pair – the public key. The private key will be kept secret. Anyone with a copy of the public key may encrypt data with it and be ensured that the owner of the public key, who also has the matching private key, is the only entity that is able to decrypt the data.

Senders can sign their messages as well. First, they create a unique fingerprint or digest of their message using a mathematical hash function. The result of encrypting this message digest with their private key is called a signature. The signature is sent along with the message. The receiver can decrypt the message and recreate the digest using the same hash function. Decrypting the signature with the sender's public key produces the original digest. If the digests match, the receiver can be certain that the message was actually sent by the signer and is further certain that the message has not been tampered with in transit. In this way, public key cryptography ensures the authenticity and integrity of communications. Since the sender cannot later deny having sent the message, non-repudiability is also ensured.

Regarding the popularity of PKI, Andrew commented that

> Until a year ago it was very hard to make people care or understand the impending widespread nature of public key infrastructure (PKI), but PKI is coming fast and it is going to be big.

A Forrester Research survey of Fortune 1000 companies indicated that only 20 % of the companies were using digital certificates in 1997, but 72% were expected to use digital certificates by 1999. Although the use of PKI in Internet security was not new, Xcert took a different approach to PKI. It aimed 'to provide a ubiquitous public key infrastructure for the Internet'. Before the existence of products such as Sentry CA, the Internet security market was dominated by large companies offering very expensive custom solutions for large corporate clients. Off-the-shelf products such as Sentry CA changed the market. Sentry CA allowed organizations of any size to issue digital certificates to its members. These organizations became their own certificate authority and issued digital certificates to their individual client base. The organization set the entry rules, allowing business on the Internet to be conducted as it is in the real world. Each organization was in charge of its own policies and internal security decisions. Pat argued that

> This approach protects privacy, because there is no centralized database where everything is stored. With Xcert's approach to Internet security, users only provide the details they need to deal with a particular organization and they only deal with the organizations they know and trust. There is no big brother watching every action.

Another potential area for the Xcert's approach is Intranets. An Intranet is a wide area network serving an organization's internal information and communication needs. Intranets are usually connected to the Internet at large through expensive security firewalls. Intranets represent the fastest growing segment of the Web technology market. Web toolmaker, Bluestone Inc., claimed that 80% of Web application development was taking place on Intranets. Xcert's technology allows organizations to control and monitor Intranet access. It also provides a measure of internal security by allowing the organizations to issue digital certificates that adhere to the organization's security standards, thus, preventing or detecting employees that access restricted information such as payroll.

Extranets also offer market potential for Xcert as organizations link electronically together. Extranets are similar to the Internet with the exception that access is restricted to only those approved organizations. An example would be a manufacturer having an Extranet with its suppliers. This network would facilitate production scheduling, delivery of raw materials and other necessary communications.

Xcert's ubiquitous PKI concept had revolutionized the industry. No longer is there a need for companies to have custom-written security systems. A company can have an Internet security system in place overnight and for a fraction of the cost of custom solutions.

Competitors/partnerships

In April 1996, Xcert announced it had won the race to hit international markets with technology that would provide secure business transactions over the Internet, using the PKI approach. Within 48 hours, Netscape issued a press release stating it would follow this technology direction. Netscape included Xcert in the list of technology partners that included GTE and VeriSign, Inc. Government agencies, organizations and financial institutions had expressed considerable interest in the Xcert's products.

Fischer International Systems Corporation (FISC) was Xcert's first major reseller partner. Addison Fischer, sole owner of FISC, was Xcert's principal investor and served on Xcert's board of directors.

Edwin Jaehne, president of FISC's technology and security services division, commented on the partnership.

> Xcert Sentry CA software is a unique solution to certificate management. The high levels of security the Sentry CA provides, along with its flexibility and ease of use, will unlock the potential of the Internet-inspired technology for a wide variety of electronic commercial transactions. At Fischer, we are now adding this technology to our proprietary products to help our clients embrace and expand their secure electronic commerce vistas.

FISC's sales force was trained to deliver the Xcert product lines to their clients. Xcert benefited from this relationship in many ways by having the ability to resell FISC products as part of a complete solution. This included consulting provided by FISC's experienced security services and technology division (FSST).

Xcert had also entered into strategic partnerships with companies such as C2 (a software company that provides secure web server software based on the popular Apache server) and Litronic (a smart card vendor whose cards seamlessly integrate with Xcert's Sentry). Xcert was also developing a distribution channel network of value-added resellers (VARs) and original equipment manufacturers (OEMs) to resell and repackage the Xcert software worldwide. In addition, Xcert had a contract with a major international technology company to provide CA infrastructure to a large Internet project.

In this era of global competition, a partner can also be a main competitor. Netscape, a partner of Xcert, was also one of its competitors. Other competitors include Entrust, Nortel and VeriSign. The biggest threat was from Entrust's Web CA product. Entrust had considerable advantages in terms of market mind share and channel leverage. In January 1997, Entrust was spun off from the secure products division of Northern Telecom (Nortel) which raised $26 million for the venture. On the other hand, the total investment in Xcert was only a fraction of that.

Xcert also had problems with a lack of leverage in negotiations because it was a 'start-up company'. In addition, the company was being used as a leverage by customers/potential partners in their negotiations with others. The image of a 'start-up company' also affected their appeal to potential employees who preferred to work for established and well-known companies.

The Internet security market, as a whole, was very competitive. It was a new market with lots of potential. There were no established companies and no established standards. Andrew stressed that

> New companies are continuously coming into the market with huge financial resources. New technologies are continuously being invented that might threaten the PKI concept. It is a jungle out there! Our goal is to stay alive, to stay competitive and to grow.

Sales and marketing

In 1996, the SoundView Financial Group estimated that the information security industry would grow from $397 million in 1996 to $4.2 billion in 2001. For the year of 1997, Xcert estimated the potential market for its type of software to be $825 million dollars. Xcert planned to use five channels for distribution (see Figure 4). They were direct 'web site', consultants, VARs, software developers and ISPs (Internet Service Providers).

To aid marketing, Xcert had hired Tim Gage as marketing manager. Tim had previously been responsible for planning and managing many European and international communications campaigns for accounts such as Artisoft, CompuServe, Fox Software, InFocus, Micrografx, SMC, Tektronix and Traveling Software.

Direct "Website"
Consultants
VARs Integrators
ISPs
Software Developers

Figure 4 Marketing channels

As a pioneer of PKI, Xcert had to pay the price. Andrew pointed out that

> The first year was spent educating the market; now Xcert has to compete against others that laid in wait and benefited from Xcert's efforts. We changed the playing field and pulled the rug out from underneath the traditional players. We said these are the rules now, this is how much we can produce for this price. And we got a very immediate reaction from all of the major players who immediately started working on products that were like ours and priced like ours.

Many of the customers the company had contacted do not feel any pressure to act quickly. In fact some potential customers came to listen to Xcert's presentation and then developed similar technology on their own. Most of the interest Xcert had received was from early adopters and companies running pilot projects. The lack of industry standards also delayed some companies' decision on security products. Many companies preferred to wait until a standard was established.

Another problem in sales and marketing was Xcert's lack of size and marketing experience. Most of the employees in Xcert were software developers. Although the company intended to hire more marketing people, this effort was hindered by the lack of financial resources. In addition, top management of large corporations preferred to do business with established companies. This had led to some interesting situations that Andrew talked about.

> We do get into situations where a large corporation, like a bank for instance, says to us that our stuff is way better than our competitors' but their management will not let them use it. We have actually had technologists say that they are going to buy our stuff and use it but tell the management they are using our competitors' product.

On a positive note, the company had found its public relations efforts to be more effective than advertising. In addition, they did not see any need to reach the end users directly. As a small company with limited resources, Xcert preferred to sell the technology rather than off-the-shelf packages.

Marketing, nevertheless, had remained a key issue faced by the management. Andrew stressed that

> We are a tiny company. We cannot afford to do R&D for the sake of doing R&D. We need to generate revenue from our R&D products and effort and we need to generate it fast.

Xcert's product line

While Xcert preferred to sell licences for its technology, it had also developed several products of its own. The Xcert Universal Database API (XUDA) was the basis for the Xcert Software Sentry suite of security enhancement products. The Xcert Certification Authority (CA), Access Control (ACL) and Pay Per View (PPV) modules had been implemented using XUDA and other products were under development.

Most of the company's development effort had been concentrated on the XUDA. An Application Programmer Interface (API) is a library of programs that can be used by programmers to develop applications. XUDA encapsulated secure database access and strong authentication via public key certificates, providing these extremely sophisticated building blocks to programmers without specific skills or experience. XUDA facilitated the development of secure applications that were server and platform independent. All of the Xcert's products were based on XUDA.

XUDA represented one of Xcert's greatest strengths, not only technologically, but from a market perspective as well. Using XUDA as a starting point, it was possible to develop a new application much faster than 'from scratch'. Several man-years of design and implementation had gone into XUDA and all of this effort was leveraged every time a new product was developed. XUDA made it possible for Xcert to respond very quickly to both technology and market changes.

Sentry CA provided a company with the ability to create a virtual private network – create a CA and issue client and server certificates – and then managed the CA with integrated administration tools. This software could be used to control access to specific information by verifying the user's identity and checking permissions on a certified access control list. It could be used to validate time-stamped transactions for internal auditing or for meeting external legal requirements. It could be used to ensure the privacy and integrity of communications between users within a virtual community as well as between users of different virtual communities. The Sentry CA could seamlessly and cost-effectively turn a public Internet site into a private Intranet site with access control. It promised to unlock the potential of the Internet for a wide variety of commercial transactions.

The ACL put organizations in charge of their own security requirements at the server level. Using secure, graphical (GUI) administration tools, server administrators could specify complete access control to various server resources. The ACL module was included with the Sentry or could be purchased separately.

The PPV Module allowed server administrators to set up PPV server resources. When a client accessed a server resource, they present their client certificate as part of the transaction. The auto-billing module saved the record of the client accessing that resource and logged it in the XUDA-compliant universal database. The software allows existing servers to be configured so user accounts (credit cards, cybercash or other means of exchange) could be automatically debited or credited based on access. This allowed costs to be associated with the material on a per-page, per-character or per-second basis.

The Xcert Software Merchant (SM) Module was built on XUDA and is used to control the download of software (or other knowledge product) over the Internet. Since digital certificates can be used to identify software components as well as human users, SMM implements and optionally enforces strong copy protection via digital certificates. To release a 30 day evaluation copy of a program, for instance, the administrator of an SMM site could specify that the certificate associated with the program expires in 30 days. To upgrade to the commercial version, it may only be necessary for the administrator to issue a new certificate with a longer validity period.

Xcert used the Xcert SMM on its own Internet site to control the download of the evaluation and commercial versions of all of its products including the SMM itself.

Table 1 lists prices for the products in the Xcert Sentry line. Included here are the CA, ACL, PPV and Automatic Billing (AB) server plug-in modules.

Other revenue streams would be from licensing the object code for XUDA to third parties for application development. Negotiations were under-way with major international corporations. Xcert also anticipated royalties from sales of third-party products, as well as from basic licence fees.

Table 1 Product pricing

Product	Price US$
CA plug-in (includes ACL)	995
ACL plug-in	295
PPV plug-in	295
AB plug-in	295
SM	1995

Note: Volume pricing is available

The road ahead

The road ahead for Xcert was bumpy. The money from the latest investor was running low and there had been little revenue to show for the state-of-the-art technology Xcert had developed.

As the two founders were both technically oriented and had little management experience, Xcert had been searching for a chief executive officer (CEO) with experience running a start-up technology company but had run into a 'Catch 22'. In order to change management, they needed money; to encourage investment, they needed to have new management in place. The question of new direction for the company complicated the search process even more. As Andrew put it,

> The company needs to decide if it wants to get additional financing or if it wants to generate revenues from an increased market share. These objectives influence the choice of a CEO. Also, there is the question of who we should have on the board of directors.

In addition, there was a question of whether to continue to run the company or to get involved in a merger or acquisition. If merger or acquisition was contemplated, whom would they select? What criteria should they use to evaluate the situation and potential candidates? What value should be placed on Xcert's technology?

Another central issue was marketing as Andrew explained.

> We have had to decide from day 1 how much and what kind of emphasis to place on marketing. Should we be hiring more marketing people or should we be hiring more systems developers now? Should we be focusing on selling the technology to software developers or should we be selling off-the-shelf software packages?

Then there is the question of branch location.

> We need to have a presence in one of the high-tech regions in the US. Investors do not come to Vancouver to look for investments. They go to Boston or Silicon Valley in California.

However, another branch in one of the expensive locations is a luxury in Xcert's current financial situation. Andrew started to ponder again.

> Should Xcert have an office in the United States or does it matter in the age of the Internet? If an office in US is necessary, should it be in Boston or Silicon Valley in California?

Suggested assignment questions

(1) Characterize Xcert's existing competitive environment.
(2) What are the management challenges that Xcert faces since the inception of the company? What are the implications of these challenges on Xcert's strategies and organizational structure?
(3) Who should they market their technology to (i.e. end users, software firms or consulting companies)? What should be the short-term and long-term marketing strategies? What are the risks? Can Xcert build entry barriers and if so how?
(4) How should Xcert manage its partnerships with other companies? Should they form strategic alliances with other companies? If so, what type of companies should they consider? What requirements should they make in their agreements?
(5) What advice would you give to Xcert regarding:
 (i) whether to open a new branch in US? If yes, which location?
 (ii) whether to hire a CEO? If so, what skills should they look for?
 (iii) the composition of the Board of Directors?
 (iv) the current financial crisis?
(6) What lesson can you draw from the case regarding the Internet security business.

Acknowledgements

The author would like to thank Dr Andrew Csinger, co-founder of Xcert Software, Inc., for providing access to the company and his help in developing the case study. The assistance of Ms Sue Rathie and Mr Kent Whitacre, who helped in shaping the case study, is greatly appreciated. Special thanks are due to Dr Chris Sauer, Dr Leslie Willcocks and the anonymous International Conference on Information Systems (ICIS '98) reviewers for their insightful comments and suggestions.

The writing of the case is supported by the International Affairs Faculty Affiliate Grant from the University of Nebraska – Lincoln and partially supported by the University of Nebraska Foundation Grant on Electronic Commerce Systems Laboratory.

Biographical note

Keng Siau is an assistant professor at the University of Nebraska-Lincoln. He holds a PhD from the University of British Columbia. His areas of specialization are information modelling methods and methodologies, WWW-based systems development, human–computer interaction and database query languages. His academic work has been published in journals such as *Management Information Systems Quarterly*, *IEEE Computer*, *Transactions on Information and Systems*, *Data Base*, *Information Systems*, *International Journal of Human–Computer Studies*, *Behavior and Information Technology* and *Information and Software Technology*, among others.

Address for correspondence

Zeng Siau, Department of Management, College of Business Administration, University of Nebraska – Lincoln, NE 68588–0491, USA.