Richard Ivey School of Business
The University of Western Ontario

9B05E002

A HACKER ATTACK: AN E-COMMERCE NIGHTMARE (A)

Carlie Bell prepared this case under the supervision of Professor Darren Meister solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

In July 2004, Joseph Roberts, the general manager of BookMart, a major online book, movie and CD store based out of Toronto, Ontario, Canada, was struggling to manage a serious breach of the company's information systems, which jeopardized both the company's reputation and its ability to provide service to its customers. Roberts had to identify how and why this breach occurred, develop an immediate plan to address the breach both internally and with BookMart's customers and the media and develop a plan to ensure the firm minimized its risk against possible future attacks.

E-COMMERCE

Since the mid-1990s when the Internet exploded into the business world, individuals and businesses have scrambled to access the information superhighway. In addition to the traditional bricks- and mortar-stores that were developing websites to attract online shoppers anywhere in the world, numerous virtual stores had flooded the Internet attempting to offer goods to customers without the high overhead costs associated with bricks- and mortar-outlets.

In its annual survey of e-commerce, Statistics Canada reported that in the private sector, the value of online orders rose 28.4 per cent from 2001 to $13.3 billion in 2002. That increase followed an 84 per cent jump in sales in 2001. However, despite the growth, e-commerce sales accounted for only 0.6 per cent of total private sector operating revenue in 2002, up from 0.5 per cent in 2001 and from 0.2 per cent in 1999.[1]

Statistics Canada reported that, for the second consecutive year, the value of e-commerce sales was highest in wholesale trade, followed by manufacturing, transportation and warehousing, and retail trade. These industries accounted for 70 per cent of all Internet sales in 2002.[2]

Statistics Canada also reported that the 2002 e-commerce market was extremely volatile, as seven firms stopped selling via the Internet for every 10 that started. Fierce online competition existed, and the market was made more volatile by consumers' lack of trust for online providers. Information confidentiality, questionable quality and service concerns were only a few of the issues e-commerce operations had to overcome, and the prediction that "e-commerce will change the world" had yet to materialize as a result of the lack of consumer confidence.

E-commerce was growing significantly, however. In the United States, the U.S Department of Commerce reported that e-commerce accounted for only 1.9 per cent of overall retail spending in May 2004, but online sales grew almost 20 per cent faster than total sales (total sales growth was 8.8 per cent whereas online sales growth reached 28.1 per cent).[3]

As consumers became more familiar with e-commerce transactions, as bandwidth improvements made product searching and price comparisons faster and more convenient, and as security and privacy issue were being addressed by both the private sector and governments, consumer confidence was rising. Numerous e-commerce sites had become trusted household names (e.g. eBay.com, Amazon.com, Chapters.Indigo.ca, BarnesandNoble.com, HomeDepot.com).

Finally, mergers and acquisitions (M&As) were common in this competitive e-commerce environment as firms that discovered a "formula that worked" attempted to expand their market share by purchasing competitors or joining forces with their supply chains.

[1] *"E-commerce Growing, but Still Tough Business: Statistics Canada," CBC News, December 4, 2003, http://www.cbc.ca/stories/2003/04/02/ecommerc_030402, July 22, 2004.*
[2] *Ibid.*
[3] *"Retail E-Commerce Growth Rate," Computerworld, June 7, 38(23) p. 48, available at www.computerworld.com, July 22, 2004.*

THE NETWORK ECONOMY ENVIRONMENT[4]

After the tragic events in the United States on September 11, 2001, awareness took on a whole new meaning, both in physical and in electronic form. People became more conscious that easily obtainable information was due to the global network economy, and how damaging that information might be in the wrong hands. Corporations responded by embarking upon new efforts to protect their employees and customers within a potentially dangerous network environment.

Apart from insider tampering, one of the biggest threats the network economy faced was "hackers," people who unlawfully and without permission gained access to corporate information systems via the information highway and the computer networks upon which the Internet is based. Hackers (also known as crackers) were divided into two groups. Hackers usually broke into sensitive corporate systems and their "claim to fame" was to either publish their "discovery" and the "how to" instructions on the web or to utilize their "discovery" to blackmail the firm by demanding ransom be paid in exchange for either not publishing or damaging the information. On the other hand, "script-kiddies" were the "wannabe hackers" who utilized the hackers' published information to break into and damage corporate systems or reputations. Script-kiddies, however, seldom understood the impact of their "games," and their favorite pastime was to deface corporate websites.

These corporate intrusions, or security breaches, could be either blatantly obvious or virtually invisible, and one of the biggest challenges faced by firms was to be able to sift through the volume of alerts to determine which were malicious and which were simply "noise." In addition to monitoring the volumes and patterns of data flow via expert systems, firms today relied upon their software vendors to inform them of alerts or patches to update their systems. Additionally, more and more firms were hiring external security testing agencies to identify weaknesses in their systems by performing security reviews, in which the consulting firm played the role of the hacker and attempted to break into corporate systems.

If a security breach was discovered, often the only way to identify the individual responsible was to have an informant in the vast "hacker underground." Some research houses and consulting firms had these networks, and could be hired to work with the damaged company and law enforcement authorities to identify the individual(s) responsible. Unfortunately, Latin America had been identified as the current "hot spot" for the hacker underground, which made it difficult for North American firms to prosecute the offenders.

These network attacks, in addition to causing system turmoil that resulted in damaged reputations and customer service interruptions, were costly. According to

[4] *"Deloitte & Touche defines the Network Economy as the business environment created by massive global communications interconnectivity and the resulting interdependent business relationships,"* *Information Security as a Business Enabler, a Deloitte & Touche brochure, Check Pont Software Technolgies Ltd., Toronto, 2003.*

the 2003 Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) Computer Crime and Security Survey[5] (a survey of 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities), the annual financial losses due to unauthorized computer use totaled more than $200 million, a figure in line with prior findings. Of this $200 million, theft of proprietary information was reported as costing more than $70 million and caused the greatest financial loss. Denial of service crimes was reported to have cost companies more than $65.6 million, and financial fraud cost these firms approximately $10.1 million. The most cited forms of attack or abuse were virus incidents and insider abuse of networks, but of those companies who reported suffering incidents, only 30 per cent reported those incidents to law enforcement.

As a result of the cost, damage and security threats associated with the network economy, governments were beginning to legislate the protection of information and data confidentiality. In Ontario, effective January 1, 2004, the province began enforcing the federal “Personal Information Protection and Electronic Documents Act” (Bill C-6), which was an effort to force companies to comply with security practices, policies and procedures that ensure confidentiality, availability and integrity of information. However, there was currently no financial penalty for non-compliance, and as corporations continued to balance the costs, risks, business productivity, and application development and integration issues, the effectiveness of this legislation remained to be seen. Additionally, three provinces created their own legislation and would enforce their own regulations as a result.

However, on an international note, in December 2000, the International Organization for Standardization (ISO) officially recognized ISO 17799 as the standard, internationally recognized, comprehensive framework for developing an effective information security management program. ISO 17799 was becoming the *de facto* information security standard, and it was a comprehensive set of best practices for information security intended to provide a common basis for developing organizational standards and effective management practices. Earning ISO 17799 certification was quickly becoming an important reliability and credibility concern for international organizations, but attaining the certificate was proving cumbersome as ISO 17799 required that organizations develop not only enterprise-wide technical and process considerations, but also human considerations and executive-level commitment.

Corporations worldwide also responded to the infamous Enron scandal in December 2001, which led to the discovery of numerous corporate greed and corruption scandals around the world. As a result, management accountability had taken on new meaning in the corporate domain. Corporate morality and integrity

[5] *An annual survey conducted and published by the Computer Security Institute, available at www.gocsi.com, accessed July 22, 2004..*

were now under public scrutiny, and businesses across North America were faced with the challenge of responding to a much more skeptical marketplace.

Finally, the “Trojan Horse” and “Blaster Worm” viruses that paralyzed industry in 2002 reinforced peoples’ sense of vulnerability, and corporations, as well as the general public, demanded greater technological security from their information technology (IT) departments and IT service providers. The blackout in the summer of 2003 across most of the Eastern United States and Eastern Canada did little to overcome this sense of vulnerability and dependency on modern technologies, especially as, in the initial days of the investigation, rumors about terrorists gaining access to the U.S. electrical grid and/or a technological virus abounded.

Businesses internationally were directly impacted by all of these events, as technological innovation, globalization, complex and rapidly changing regulations, and increased senior management and boards of directors’ accountability combined to alter the risk-management landscape. Additionally, customer skepticism reached an all-time high, causing increased e-commerce competition based on price, quality, service and reputation wars.

To protect themselves against possible security attacks and to meet the demands of the altered global environment, e-commerce firms responded with stricter and more publicized security measures. Intrusion detection systems, strict password and personal identification number (PIN) log-on requirements, and access control software to ensure customers had access only to the public network and not to the internal private network (which supports internal business environment activities) or the semi-private network (which enables customer service agents to enter the public server from the private server in order to assist customers with technological and order issues) were implemented and publicized, and e-commerce growth continued.

IT AT BOOKMART

Like many of the large retail e-commerce sites, BookMart had achieved growth in part through numerous mergers and acquisitions (M&As) with small and medium-sized book, CD and video virtual sites. Most recently, in October 2003, BookMart had merged with a medium-sized virtual music site and had acquired an up-and-coming online sport video operation. BookMart had earned its online reputation not only through the quality of its products and service, but also due to the loyalty program it had initiated and maintained. As customers purchased books, videos or CDs, points were awarded, which could then be redeemed for discounts on future purchases. The recent merger and acquisition were particularly enticing for BookMart as both firms had their own loyalty programs, similar to BookMart’s. However, the merger of the loyalty programs required special attention so that customers could retain and utilize points previously earned, despite the conversion required to ensure the points allocated were consistent with BookMart's own generous formula.

Lois Fairchild, BookMart's Chief Information Officer (CIO), and her IT team were responsible for integrating the variety of IT equipment and platforms that resulted from the numerous M&As by their respected deadlines, maintaining the point-of-purchase (POP) systems, designing the corporate and catalogue web pages (including the BookMart home page, online technical support pages, customer order pages and BookMart's own site search engine), enabling the storage, delivery and retrieval of e-mail for their employees and the delivery of e-mail to their customers, as well as developing BookMart's in-house IT systems (i.e. maintaining the systems and providing end-user training and support to BookMart's employees, including those who responded to the 24-hour customer support telephone lines). Overall, Fairchild was responsible for overseeing 72 IT personnel, who were divided into four teams: web development, internal customer support, external customer support and internal maintenance.

Fairchild was very conscious of the numerous privacy and security measures necessary for online operations, and she and her IT team had implemented many security measures to protect the firm. Both BookMart's employees and their customers ultimately had access to the same connected system (due to the semi-private network that connected the private network to the public one), but employees' and customers' access to certain system components, as well as the resulting security/privacy and the IT department's ability to influence and control those measures, were different. As a result, in addition to the access controls in place, Fairchild had assigned security measures to the internal IT maintenance team.

In addition to constantly patching and updating their virus scanners, firewalls (intrusion detection systems) and software programs as soon as the vendors made the IT team aware of new releases or alerts, BookMart's internal IT maintenance team took measures that were standard in the industry. Each employee had a unique user name and password to log into and out of BookMart's systems. Emphasis during training (by the internal customer support team) ensured employees were careful to guard this personal and private information, and employees were also encouraged to change their passwords regularly. Although Fairchild's training team had explained the need to ensure passwords weren't easily identifiable (using dates of birth or family names is predictable, and common words might be picked up by hacker software that uses the dictionary to identify passwords), it was difficult to ensure that employees carefully selected, routinely changed and remembered, their passwords.

For months, the IT team had been considering assigning randomly generated passwords, but discussions with employees resulted in very negative reactions to this proposal. The biggest concern appeared to be that employees feared their inability to remember the assigned, ambiguous passwords, and given that the IT department had proposed that passwords be changed quarterly, employees feared that their work would be disrupted due to the complexity (and therefore lack of memorability) of the ambiguous passwords. Additionally, the internal IT customer support team was already overwhelmed with meeting their users' needs, and felt they were unable to respond to the increase in assistance that would be required if users forgot their password.

External customers were assigned ambiguous user names and passwords by the external IT customer support team and were reminded through monthly e-mails to keep that information private and secure. Customer credit card transactions were secured using Secure Socket Layers (SSL) encryption technology, which prevented information from being intercepted and read as it was sent over the Internet to BookMart's own servers. The external customer support team was trained by the internal IT customer support team to be extremely cautious when utilizing the semi-private network to assist customers with orders or technological issues, especially with regard to user names and password communications.

According to Fairchild, BookMart's systems were well secured, and the security and privacy policies in place were more thorough than the industry standard.

THE DILEMMA

At 10 a.m., on Friday, July 9, 2004, Roberts was in the middle of discussing BookMart's preliminary financial forecasts for the upcoming 2005 fiscal year with Tim Wilson, the vice-president (VP) of finance of BookMart, when they were abruptly interrupted. Lois Fairchild rapped on the door and rushed into the room. Her face was flushed, and she appeared panic-stricken. Fairchild reported that one of BookMart's customers had just telephoned BookMart's support line to inquire why BookMart's home page seemed to be displaying a list of peoples' names and their contact and billing information on his computer. Fairchild proclaimed that she was forced to shut down the entire network system until it was secured.

Fairchild explained that a hacker must have broken into the network, most likely due to a weakness in BookMart's multi-platform architecture, but what exact damage the hacker had caused would take weeks, maybe months or even years to discover. Fairchild knew that the hacker had broken into BookMart's semi-private network and had managed to make BookMart's customer information, internal human resources data and the firm's accounting records visible to anyone on the web who found BookMart's home page. Until they were able to ensure the privacy of this information, Fairchild had no choice but to shut down information systems (IS) to protect customers' private information (including credit card and bank account information) and the company's assets and employee information (social insurance numbers, salary information, and the company's own banking statements and account numbers, as well detailed accounting records). Unfortunately, it was difficult to tell if the hacker had tampered with any of BookMart's other files or systems in the process, and discovering the hacker's exact path through the system was almost impossible. As a result, if the hacker had altered or damaged any of BookMart's files, it may only become evident as time progressed and errors were discovered and reported.

Roberts and Wilson, recognizing the seriousness of this problem, demanded more information. How was this possible? What damage did the hacker do? How should BookMart protect itself against possible future attacks? How long must the system be shut down? What should BookMart tell its customers? Fairchild didn't have all the answers yet, nor was she entirely certain about what to do — she was certain the systems were secure!

As Roberts and Wilson listened to Fairchild, it became obvious that BookMart might be in serious trouble, legally, financially and reputationally. As Fairchild rushed out of the office mumbling something about "how on earth could this happen," the telephone rang. Roberts looked at Wilson hesitantly as he answered. It was a reporter from Canada's leading business newspaper, the *Globe and Mail*, calling to confirm that BookMart's systems had been attacked. Roberts opened his mouth and began to speak.