Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2007 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2007

# The Magnitude of Switching Costs for Corporate Antivirus Software Switching Decision

Cheng-Yu Hou
*National Taiwan University*, d93725009@ntu.edu.tw

Ching-Chin Chern
*National Taiwan University*, chern@im.ntu.edu.tw

Yu-Tzu Lin
*National Taiwan University*, d94725009@ntu.edu.tw

# 77. The Magnitude of Switching Costs for Corporate Antivirus Software Switching Decision

Hou, Cheng-Yu
National Taiwan University
d93725009@ntu.edu.tw

Chern, Ching-Chin
National Taiwan University
chern@im.ntu.edu.tw

Lin, Yu-Tzu
National Taiwan University
d94725009@ntu.edu.tw

## Abstract

*Today's businesses environment is forcing companies to become increasingly more efficient in applying Internet technology to conduct transactions. AS the possibility of infection by computer virus is much greater now than ever before, businesses search for appropriate corporate antivirus software to safeguard their computer systems. This paper considers corporate antivirus software switching as one of the major security selection problem and proposes possible avenues for software switching decision and management.*

*In conceptual model, we draw upon switching costs where transaction costs, learning costs, and artificial costs were examined as main costs for software switching decision. Our findings shown only two out of three types of switching costs have influence over corporate antivirus software switching decisions. Despite the existence of switching costs, businesses continue to repeat software switching because the perceived risks of security threats are much greater than the switching cost itself. Furthermore, we examine various approaches to the cost of switching and then propose an index map to evaluate switching decision. Five sets of propositions are advanced to help guide this research.*

**Keywords:** Corporate antivirus software (CAV), Information security, Switching costs, Service switching

## Introduction

Constructing an e-commerce business environment using information technology (IT) has become a growing trend in corporation governance. More and more businesses are using the Internet and computer systems as the basis to develop their business application, e.g. Electronic Banking and Virtual Personal Network service (VPN). However, the Internet is an open cyber environment. These applications are typically exposed to security threats such as computer virus, worms, and Trojans. These security threats cause damages to the computer systems and put the systems' privacy in jeopardy.

Computer viruses have become an ongoing world problem and can travel quickly through the Internet, causing even more destruction. According to a survey from Computer Security Institute, businesses financial losses due to security breaches have escalated to $140 million dollars in 2004; of which the biggest losses was caused by computer viruses (Gordon et al. 2005). More recently, a survey by the Department of Trade and Industry in the United Kingdom found that 88 percent of businesses had been affected by computer viruses in 2005 (Potter 2006). In the next five years, viruses in hybrid and advanced forms are expected to continue to have a large-scale impact on all kinds of businesses, such that protecting businesses against viruses attack will be harder than ever (Robbins 2004).

In the fight against these viruses, the best solution is to utilize appropriate corporate antivirus software (CAV). The software providers offer numerous CAV to meet businesses' security needs, ranging from simple virus protection program to more sophisticated and complex antivirus program. Although the instillation rate is near to 100 percent, there is no software that guarantees full protection against all virus threats (Keller 2005). For added protections, businesses tried to install two antivirus packages on one PC. Nevertheless, it is infeasible to do so because of two different antivirus packages disrupt each other's functions (Kaspersky 2005); thus, if a business finds its current CAV short in meeting its requirements, it can switch to a new CAV provider. When businesses activate the mechanism of switching CAV, it considers the switching costs as vital factors.

Earlier works demonstrated that the switching costs were significantly related to software switching decision. Businesses were often locked into specialized software, which caused difficulty in finding a replacement (Laudon 2000; O'Brian 2004). It is interesting that scholars noted that the most businesses emphasized the features and effectiveness provided by antivirus software, rather than the cost factor (Hubbard 1998; Liu 2003). This argument shows that, in practice, the reasons for switching security software are different from the reasons for switching other application software. There seems to an understanding that security software is fundamentally unlike from other application software used by businesses. Additionally, the IDC annual report found that the market share of antivirus providers changed every year, suggesting that businesses switched CAV under some conditions that we currently do not know (Burke et al. 2004). Since serious lack of study reported in this issue, the goal of this paper is to provide an understanding of the why businesses switching CAV and how do switching costs affect the CAV switching decision.

To better understand this issue, this paper development a conceptual model grounded in Klemperer's switching costs view in conjunction with transaction cost theory and examined this model on a deeply multi-cases data. The contribution of this paper has three folds. First, we seek to fill this gap of studies in the topic of switching cost related to security software, in particular the CAV switching. Second, we provide guidelines that businesses can follow when making decisions about switching CAV. Finally, we proposed an index map for IT executives to ensure switching options. In addition, researchers can base the questionnaire of index map to develop future studies in quantitative method.

The rest of this paper is organized as follow. Section 2 contains observations on the state of antivirus industry and a concise literature review on switching costs. Section 3 proposes a conceptual model of CAV switching, and describes the methodology uses in this research. Section 4 describes the profiles of the cases, and Section 5 assesses the results of the study and lists the research propositions. Finally, proposed an index map for practitioners to assess switching among CAV, more, implications for researchers and practitioners are drawn.

## General background

### *Setting: The Antivirus Software Industry*

The development of the antivirus software industry has begun in the early 1990s. Antivirus providers can be divided into three groups based on their market share. They are: industrial leaders, second-tier providers, and others that have no significant impact in this market. Table 1 shows the leaders and one company of the second-tier providers (Kaspersky 2005). Among the leaders, Symantec, McAfee, and Trend Micro, severely engage in marketing and after-sales activities that significantly affect the market. Second-tier companies are providers whose market share is substantially lower than those of the three leaders, even though their

annual income amounts to tens of millions of dollars. The majority of such providres has a significant presence in their respective domestic markets, but a relatively small presence in foreign markets. Sophos, the most successful antivirus provider in the UK, is an example of a second-tier providers. Finally, the "other" providers category includes several dozen companies, most of which only engage in their respective domestic markets. In 2004, the total market for antivirus solutions was worth $3.7 billion, compared to $2.7 billion in 2003 (Burke et al. 2004).

**Table 1: Income and Market Share of CAV Providers**

| | Annual income | | Market share | |
|---|---|---|---|---|
| Company | 2003 | 2004 | 2003 | 2004 |
| Industry leaders | | | | |
| Symantec | 1098 | 1698 | 28.3% | 35% |
| McAfee | 577 | 683 | 22.6% | 14% |
| Trend Micro | 382 | 587 | 12.4% | 11% |
| Second-tier companies | | | | |
| Sophos (UK) | 97 | 156 | 2.1% | 3% |

## *The State of the Antivirus Software Industry*

Businesses usually choose antivirus software because of their technological characteristics. The most important consideration is a comprehensive virus protection offered by the CAV (Liu 2003). There is relatively few software in the market that offer 100% protection. In fact, the majority of antivirus software guarantees less than 90% protection; hence, insufficient protection is the most important problem faced by both users and the antivirus industry.

Kaspersky (2005) found several issues related to insufficient protection. First, some antivirus providers are unable to update their 'antivirus signature' immediately after a new virus is detected so that computer systems are defenseless against attack. Second, some software can not detect certain viruses when they attack computers, which imply that the software are inferior and can have a strong negative impact on business. Third, some software is more hardware resource required, thus caused the computer system in a poor performance when install a specific antivirus software. Finally, it is currently infeasible to install two different antivirus packages on the same computer to increased protection due to compatibility issues.

The characteristic of CAV differs from other application software, and these differences have distinct implications for customer satisfaction and intention to switch CAV service. First, CAV need regular signature up-to-date for comprehensive protection. Running antivirus software without the latest updates exposes computer systems very rapidly to attack by the latest threats. Second, the service is constrained by the term of contract validity. Antivirus service requires annual renewal with original service provider for the newest signature update service. Third, CAV comprises two components: the antivirus servers and the clients. CAV has to install on antivirus servers first (may not only one but at least two servers for disaster recovery), then deploy to all clients inside a business by local area network. Thus, IT staffs have to learn the operational skill about installation, configuration the antivirus servers and deployment CAV in all clients within business. Finally, it is impossible to install two distinct antivirus packages in same PC to increase protection due to they distribute each function and cause computer system unstable. Therefore, if a business finds its current CAV have been unable to stem the increase virus attacks on computer systems, it can switch to a new CAV provider.

### *Switching Costs and Service Switching*

Switching costs refer to the costs of switching from one product to another competing product (Porter 2001). Giving the results of O'Brian (2006) study in office automation, switching from the Microsoft Office suite to the competing StarOffice suite, which may cost less in software itself but imposed a higher switching costs on users, who were accustomed to the functions and file formats of Microsoft Office. In another word, the higher the switching costs, the more difficult it is to switch brands even though with low adoption costs; hence, switching costs is viewed as a vital strategic element in the marketing arena. It has been suggested that switching costs will affect prices, market share and also linked to a variety of competitive phenomena, such as pricing wars and large discounts offered by businesses to attract new customer (Klemperer 1987, 1995; Chen and Hitt 2002; Fornell 1992).

Reasons to switching include the economic, functional, and emotional sacrifices that may be necessary before, during, and after service conversion. Klemperer (1987) divided switching costs into three categories: transaction costs, learning costs, and artificial costs. In awareness of transaction cost's definition, we must further explore transaction cost theory to investigate the origin of such cost. Transaction costs are incurred when customers switch suppliers, because finding new suppliers involves the processes of searching for and evaluating alternative products. If a business decides to switch current software, the firm has to search for a new supplier and evaluate the supplier's reputation. The process of finding and evaluating a new supplier generates extra tangible and intangible expenses, which called transaction costs. Williamson (1985) extended Coase's (1937) concept and defined four important attributes of transaction costs, namely, "bounded rationality", "opportunism", "uncertainty," and '"asset specificity". Bounded rationality is that economic actors try to be rational, but they are limited. On the other hand, economic actors are inability of human mind to find or process all the information about a transaction; therefore, it is conducted with a certain level of uncertainty. Opportunism refers to the economic actors' tendency to be motivated by self-interest, which makes allowances for guile. Because of these two underline assumptions, there is uncertainty about transaction's future, including ex ante and ex post uncertainty. Finally and important one, Williamson defined asset specificity as: "The degree to which an asset can be redeployed to alternative uses and by alternative users without sacrifice of productive value", thus, when a transaction requires highly specific investments (asset specificity), there must be a mechanism to protect the investor. This paper defined assets specificity in CAV switching as physical IT hardware and system software request.

Learning costs relate to the effort customers must expend to reach the same level of comfort with a new product that they had with their previous product; for instance, when a business switches to an ERP application from SAP to Oracle. Users must learn about these new functions and operating skills since the functions of Oracle's system are different to those of the SAP system, which can be seen as learning costs. Finally, artificial costs are the costs related to what the business does to retain its existing customers – for example, frequent flyer miles provided by airlines (Klemperer 1987, 1995).

Much effort has been conducted to study the effect of customer satisfaction in on-line service switching. Consumer satisfaction will influence service continuation or service switching (Kim et al. 2006). The selection of antivirus and content filtering software has been measured in six criteria including: installation, operation, administration, notification, antivirus, and content filtering (Mamaghani 2002). Except for content filtering, the other five criteria are used in evaluating the satisfaction of CAV service, and to identify the reasons why business switches their CAV service.

## The Conceptual model and methodology

### *The Conceptual Model*

Consistent with our research purpose of studying the switching CAV, we have followed a detailed and precise theoretical and conceptual model illustrate in figure 1. We specify the intention to switching CAV as the dependent variable. From economic perspective, that views switching behavior primarily in terms of motivation to switch CAV service, and the switching decisions are made by evaluating three types of switching costs. We identify motivations to switch CAV service as an independent variable. Transaction cost, learning cost, and artificial cost were the three modulators that influence the intention to switching CAV service. These three modulators were adapted from Klemperer's switching costs, which is widely applied to analyze IS/IT switching phenomena (Chen and Hitt 2002; Kim 2003).

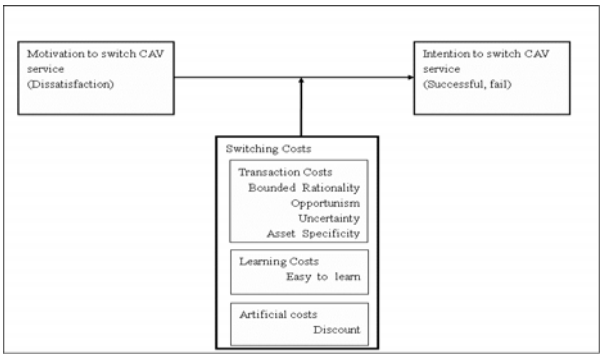


**Figure 1: Conceptual model**

After the completion of the CAV switching decision process, a business faces two choices: switching to new antivirus provider, or keeping working with the existing one. The switching activity is defined as "successful" for the condition that a business decides to switch to a new provider. Oppositely, if a business continues to work with current provider, the switching activity is defined as "fail".

### *Methodology*

Delving into CAV switching literature, there has been no related works and might be considered as a new topic in research of information security. For such reason, more exploratory studies are needed before a theory can be formed. The Case study approach was selected for this research as this approach lends itself to concentrated focus on the issue, and accommodates several data-gathering techniques. A survey of business users on this topic would not be appropriate because the terminology and some of the concepts are still being formulated. Besides, business users are less likely to divulge highly sensitive data about information security in a survey and send it to a stranger (Kotulic et al. 2004). Therefore, we adopt a preliminary research method, case study, most appropriate for exploratory and explanatory research since they are able to capture a depth of details on the subjects.

Researches used case study approach as their research strategy in the Information System discipline (Hsieh 2002; Kern 2002; Khalfan 2004). The case study approach refers to an in-depth study or investigation of an existing phenomenon using multiple sources of evidence within its real-life context (Yin 1994). The research approach can be used for a single case based on thorough observation of a case and in depth details about the subject, or for multiple cases with multiple-factor findings and a cross-analysis that can result in the development of a theoretical framework (Eisenhardt 1989). This paper used the case study methodology with multiple cases and develops a set of propositions based on these cases' findings.

Of the four organizations, one academic institution and three businesses were selected as case studies for this research. The network administrators, chief information security officer (CISO), and security staffs of these businesses were the key personnel interviewed. Construct validity was established by triangulation, chain of evidence and formal review by the interviewees for verification (Yin 1994). This paper gathered data via notes, documents, and one-on-one interviews. The interviews were conducted semi-formally, with one researcher talking to one representative of the case businesses. Each interview included questionnaire was as follows: Profile of the case, the business's antivirus budget, the reasons for switching CAV, as well as the switching costs involved in and influence on the switching decision-making process. Five possible responses were provided (strongly agree, agree, natural disagree, strongly disagree). In the next section, the background of the four businesses will be described and the results of the decisions they made in CAV switching will be thoroughly reported.

## *Cases Profiles*

Several criteria were settled to select for appropriate cases: the size of the organization; its experience of CAV switching; and the industry of the organization. In terms of size, the size of these four cases range from small-sized organizations, which employ 300 to 500 people; to medium-size organization, which employ over 1000 people. The size of organization implicates the information capability; that is, the large an organization, the more critical its information security issue. Therefore, a medium-size organization tends to pay more attention on the information security issue than a small-size organization.

Of the four cases that we contacted, each one had its experience in the activity of switching CAV. In order to apply our findings to a broader condition, the cases were drawn from distinct industry sectors: academia, telecommunication, and manufactures. The data was gathered between July and November 2005, with follow-up interviews in the early 2006. We will briefly describe the four cases and cases' details in Table 2.

**Table 2: Detail of Cases**

| | Case A<br>M University | Case B<br>V Telecom | Case C<br>F Electric | Case D<br>S Tech |
|---|---|---|---|---|
| Industry sector | Academia | Service | Manufacture | Manufacture |
| Number of clients | 1100 | 750 | 300 | 200 |
| Original use CAV | Symantec | Symantec | Trend Micro | Trend Micro |
| Switching to CAV | Trend Micro | McAfee | Symantec | Symantec |
| Switching results | Failed | successful | Successful | Failed |

Case A: M University

M University is a prestigious University in Taiwan. As the end of 2005 equipped with 1,100 networked PCs. M University had evaluated to switch to Trend Micro but the activity failed. Therefore, it will be used as a failed switching case.

Case B: V Telecom

V Telecom is one of the three leading telecommunication companies in Taiwan, which provides 3G communication services. It employed over 750 employees. It has successfully switched its CAV from Symantec to McAfee in 2003. This case is used as an example for a successful switching experience.

Case C: F Electric

F Electric was the leading heavy electrical engineering equipment in Taiwan. Its main

products are high-voltage transformers, and it is a certified supplier of General Electric in the US. The company switched CAV from Trend Micro to Symantec successfully once in 2004, and thus used as the second successful example in this research.

Case D: S Tech

S Tech is a manufacturer of IT equipment accessories. It supplies world famous brands, such as Fuji and Sony, with cases for consumer electronic products. To deal with 'Blaster' virus outbreak, S Tech switched to Symantec CAV temporarily and removed it soon after the crisis had passed. We use S Tech as another failed switched case.

## Discussion

### *Switching Reasons*

In regard to the switching reasons, we found 'sustained dissatisfaction' as the main reason that motivates businesses to switch CAV. Four Cases' switching details show in Table 3. M University intents to switch CAV that resulted in a series of continuous attack by worm-type viruses, e.g. "Nimda", "CodeRed" and "Blaster". As Symantec did not provide adequate protection, every virus breaches has make great impact on the business which normally lasted for about a week and thus resulted in an enormous operating losses. Hence, the business was then motivated to switch to new CAV to obtain adequate protection.

**Table 3: Reasons of switching**

| | Reason of Switching | Description |
|---|---|---|
| M University | Dissatisfaction | Unable to stop virus attacks |
| V Telecom | Incompatibility | With new e-Mail system |
| F Electric | Dissatisfaction | Hard to administrating clients |
| S Tech | Dissatisfaction | Unable to stop virus attacks |

In contrast, V Telecom switched their CAV due to incompatible with their new e-mail system, MS Exchange 2003, which provided higher security level of e-mail service. As McAfee's CAV was the only package that supported the function of content filtering of the new e-mail system, V Telecom had no choice but to switch to McAfee for their security needs.

To summarize, we found that businesses switch their CAV due to 'sustained dissatisfaction'. The sustained dissatisfaction was caused by continuous virus breaches. If a CAV cannot protect a business from computer viruses attacks, its daily operations could be affected, and the business would be encourage to switch CAV. Hence, we propose the following proposition regarding the businesses' intention to switch their CAV.

**Proposition1**. The greater degree of business dissatisfying with current CAV performance, the higher frequency they switching to a new provider's CAV for effective protections.

### *Transaction Costs of Switching*

*Effect of bounded rationality*

In this research, 'bounded rationality' was determined as how many CAV packages a business evaluates before it switching to a new provider. For instance, if a business evaluates all CAV in industrial leaders before making a decision to switch from Symantec to McAfee; then we say its decision was not limited by bounded rationality. On the contrary, if a business evaluates only Trend Micro before making any decision, its decision has been limited by bounded rationality.

M University originally implemented Symantec as its CAV. When the Chief Information Security Officer (CISO) motivated to switching CAV, it evaluated only Trend Micro, a competitor of Symantec, rather than considered all providers in the industry leaders. Consequently, it is limited by bounded rationality.

V Telecom was the only business that evaluated all CAV before making a switching decision. In late 2003, V Telecom implemented MS Exchange 2003 as new e-mail system, but the Symantec CAV used at the time did not support content filtering on MS Exchange 2003. It means that the Symantec was incompatible with the new e-mail system. Therefore, V Telecom had to search another CAV to fit into the MS Exchange 2003. It surveyed all other providers in the industrial leaders- including Trend Micro and McAfee- before making a decision to switch from Symantec to McAfee. Hence, V Telecom was not limited by bounded rationality.

F Electric switched from Trend Micro to Symantec, because they were not motivated to evaluate another CAV. They selected Symantec because it was the leader in antivirus industry. This decision was based on the product's market share and the provider's reputation. Thus, 'no motivation' to evaluate other CAV was the main driver of Case C's decision, which was also limited by bounded rationality.

S Tech switched CAV because of the 'Blaster' virus outbreak erupted during 2003, which impact on its daily operations. Hence, the CAV switching decision had to be made within a short time in order to recover from the virus outbreak. To address the problem, the CISO decided to deploy Symantec's CAV on all clients, but switched back to the previous CAV when the crisis had passed. Because it did not evaluate all CAV in the industry leaders when making the switching decision, S Tech was limited by bounded rationality.

*Effect of Opportunism*

Opportunism is more than the simple defense of one's interest or value maximization; it is self interest seeking with guile (Williamson 1985). Thus, in this paper, opportunism refers to a provider's intention to promote CAV to customers regardless of their software fitting with customer or not. We found that opportunism was evident in the two cases where CAV were purchased from authority resellers (contacted with providers), but the other businesses procured CAV from their long-term IT resellers, and implemented the software by themselves. Our findings indicated that opportunism did not have any effect on a business decision-making process when the reseller could not contact their customer directly and support the opportunism is one behavior assumptions of transaction cost theory.

The reseller of Trend Micro promoted the CAV to M University aggressively and tried to finalize the deal as soon as trial CAV was installed. However, M University's CISO concerned the reseller's IT staffs could not implement the software properly due to lack of experience, but the reseller debated that the CAV was easy to install, no matter how large the business. This assurance of the sales team implied that Trend Micro tries to sell its CAV to a customer regardless customer's needs and thus opportunism existed in M University.

In V Telecom, the sales teams from Trend Micro and Symantec tried to sell their CAV by promising to solve any problem after deal, even though both sales teams had known that their packages were not fully compatible with the MS Exchange 2003. The promises implied the sales teams tried to promote CAV regardless customer needs. This promise was a sign of an opportunistic behavior and V Telecom was another case to prove that opportunism occurred

in the contacted with providers.

By contrast, the switching decisions of F Electric and S Tech were not affected by provider's opportunistic behavior due to they did not get in touch with the providers. Thus, the providers' sales teams could not deal the businesses to promote their products directly. F Electric and S Tech decided to switch CAV based on provider's good reputations; purchased software from their long-term IT suppliers, and deployed the software by IT staffs.

*Effect of Uncertainty*

Adopting CAV in a business is like outsourcing an information security service to a provider for protecting its in-house IS. Accordingly, we can use the software outsourcing perspectives to examine the uncertainty in CAV switching decision. Uncertainty about software outsourcing is caused by unclear specifications, scheduling delivery dates, and budgetary problems (Wang 2002).

When evaluation the CAV switching, the M University's CISO emphasized on the reseller's ability to deploy the CAV in a large network environment because of its complex network infrastructure, which consisted of Ethernet, Giga Ethernet and wireless. However, the CISO took two months to evaluate two resellers authorized by Trend Micro. He found neither of the two resellers had experience in deploying CAV in larger and complex network infrastructures, and only realized that it was impossible to find any qualified reseller. For this reason, the CISO decided that is too risky to make a switching decision because this transaction implies high uncertainty then decided to call off the switching activity. Due to lack of qualified reseller before the procurement deadline, he decided to remain with the existing reseller who had experience in implementing Symantec CAV in large network environment.

The others cases perceived low uncertainty when switching CAV. In V Telecom, because of the provider's reputation and consultant's experience for the new e-mail system, lower the uncertainty. The provider, McAfee, enjoyed a good reputation in the antivirus industry and was recommended by the consultant as being the only solution fitting with MS Exchange 2003. Moreover, V Telecom pre-tested the McAfee CAV before implementation to iron out any problem in order to reduce the uncertainty involve in the CAV switching.

*Effect of asset specificity*

The CAV composed of two components: the antivirus servers and the clients. Software has to install on antivirus server then deployment to all clients by local area network. This study defined assets specificity in CAV switching as physical IT hardware and system software requirement in both servers and clients. All providers' antivirus servers can be installed on X86 PC and run in the Microsoft Windows-based platform as showed in Table 4.

**Table 4: System requirements for different antivirus software**

| | Symantec | Trade Micro | McAfee |
|---|---|---|---|
| Hardware Requirements | 64 MB RAM<br>111 MB of disk space<br>Intel P200 MHz above | 128MB of RAM<br>300MB of disk space<br>Intel P200 MHz above | 32MB RAM<br>38MB of disk space<br>Intel P166 MHz above |
| Software Requirements | Win 2000 Pro. or above<br>Web server: MS IIS Server | Win 2000 Pro. or above<br>Web server: MS IIS Server | Win 2000 Pro. or above<br>Web server: MS IIS Server |

In order to centralize management all clients, M University installed Symantec server-site on two X86 PCs to support over 300 clients. V Telecom and F Electric installed the antivirus

servers on X86 industrial PCs in order to compatibility with existing IT hardware. S Tech used only secondhand X86 PC to be the server. According to these findings, the antivirus servers can be installed on the existing hardware platform even businesses switching to new CAV. It is not necessary to buy additional hardware or system software (operating systems) when switching to new CAV, showed low asset specificity on CAV. The clients are available for Windows, Linux, Netware and Novell; various platforms operating on desktops. Therefore, the effect of assets specificity is not significant in clients too, which leads us to the following proposition.

**Proposition 2**: The lower asset specificity regarding the CAV, the higher frequency business switches their CAV without "lock-in".

### *Learning Costs*

For the necessary of regular up-to-date service, businesses adopting antivirus service are likely to outsource a software project or service to antivirus providers. It is appropriate to evaluate the CAV service by software outsourcing criteria. Wang (2002) defined specific skill learning in software outsourcing as "the unique skills, functions, and business knowledge required for completing the software outsourcing project". Thus, this paper defined skill learning of CAV as the unique skills and antivirus knowledge required for implementation and maintenance inside the business.

This paper refers the learning costs caused by a CAV switching decision as the degree of difficulty involved in unique skills and antivirus knowledge required to implementation and maintenance a new CAV inside the business. We comment the learning cost is high if it takes the IT staffs a long period of time to acquire the skill. Oppositely, the learning cost is low if the IT staffs can acquire the skill quickly.

**Table 5: The effect of switching costs on cases**

| | Transaction Cost | | | | Learning Cost | Artificial Cost |
|---|---|---|---|---|---|---|
| | Bounded Rationality | Opportunism | Uncertainty | Asset specificity | | |
| M University | × | × | × | - | - | × |
| V Telecom | - | × | × | - | - | × |
| F Electric | × | - | - | - | - | - |
| S Tech | × | - | - | - | - | × |

**× = Significant, - = Not significant**

Table 5 illustrated the results of four cases, whether switching CAV was successful or not, they all experienced low degree of difficulty involved in learning. Essentially, the CAV is designed to detect and remove viruses, and thus the user interfaces and required operating skills are similar to each other. Consequently, the IT staffs do not need long-term training to maintain new antivirus software. For example, even thought F Electric and S Tech had no assistance from antivirus resellers, both were able to deploy new CAV quickly. The findings illustrated difficulty level required in installing and operating various CAV is low. Hence, we put forward the following proposition regards to the learning costs.

**Proposition 3:** The lower level of operational skills is experienced by businesses, the higher frequency switching to a new CAV.

### *Artificial Costs*

Artificial costs are business costs that incurs to retain its exiting customers or to attract new ones. The costs originate from the sales strategies employed by the existing provider and the

new provider involved in a firm's switching processes. To identify such costs, researchers need to distinguish the sales actions in the switching proceeding of antivirus software. Consequently, we found that, to reduce/increase artificial costs, providers offer free upgrades, free trials, price discounts, free training, and free deployment. Table 6 summarized the findings about the artificial costs in four cases.

**Table 6: Artificial Costs**

| | M University | | F Electric | | V Telecom | | S Tech | |
|---|---|---|---|---|---|---|---|---|
| | Existing | New | Existing | New | Existing | New | Existing | New |
| Upgrade | Y | Y | Y | Y | N | Y | Y | Y |
| Free Trials | Y | N | N | N | N | N | Y | N |
| Discount | Y(more) | N | Y | Y(more) | N | N | Y | N |
| Free training | Y | Y | Y | Y | N | N | Y | N |
| Switching decision | × | | | × | | × | × | |

**"Y" Did, "N" Did nothing**

The existing antivirus provider of M University, Symantec, offered more benefits than the alternative provider, Trend Micro. Trend Micro offered only one month trial CAV and a half-day training session for the IT staffs, the Symantec offered an upgrade of the CAV, which supported more features for client protection (e.g. an incoming e-mail scanning for virus detection), and a trial software of e-mail gateway. Furthermore, the Symantec offered unlimited trial and price discounts as incentives to secure M University's business. Symantec offered M University better deal than Trend Micro, M University decided to continue with the Symantec and signed a two-year contract, which allowed them to upgrade to a new version of the CAV. In case of V Telecom, a well-known business in Taiwan, its antivirus policy will be a template for others. The new provider, McAfee, offered CAV with a low price in order to have a successful case in the Taiwan market as an advertising to attract other businesses. That is, McAfee hoped for increase in revenue from other businesses. Also, the existing provider, Symantec, offered V Telecom a big discount too. In addition to McAfee CAV's lower price, and it was the only compatible with the new e-mail system; thus, V Telecom decided to switch to McAfee. In this case we found again, pricing is an important factor that affects CAV switching decisions; low price implies lower artificial costs.

F Electric had procured new CAV from a long-term supplier when they decided to switch CAV to the Symantec, and it was deployed by F electric's IT staffs. The company's CISO commented that the major switching costs were generated by man hours of artificial cost to deploy the new software on all clients inside the business. Another example is the S Tech, they deployed Symantec CAV to recover form a worm-type virus outbreak, and latter remove it and reinstalled Trend Micro CAV on all clients due to still one more year contract with Trend Micro. While the Symantec was going to terminate the contract with S Tech, Symantec only called about repurchase, but Trend Micro offered more than Symantec, e.g. Price discount, Trial software, and free antivirus training for IT staffs, to increase S Tech's repurchase intention. Likely the CISO of F Electric mentioned above, the S Tech's CISO pointed out the major artificial costs was incurred by installation cost; e.g.: installed Symantec software on all clients and remove Trend Micro, re-installed Trend Micro on all clients then remove Symantec.

**Proposition 4:** The more sales strategies are adopted by the provider to reduce the artificial costs, the higher frequency businesses switching to the provider's CAV.

Installation cost is a vital element within artificial cost which businesses have to consider in CAV switching. In spite of switching results, successful or failed, the installation cost were

occurred in the CAV switching process because the four cases surveyed in this study were experienced installing antivirus software on all clients. Therefore, we proposed the following mathematical equation to calculate setup cost within artificial cost when switching CAV: $C_r = C_h * Q * T + \alpha$ where $Cr$ denotes the total installation costs, $C_h$ denotes the cost per man hour, $Q$ is the number of clients in the business, $T$ is the time spent per client installation, and $\alpha$ is a firm-specific fixed cost in businesses. According to this equation, the installation cost is directly related to the number of clients within the business; that is, a firm with more clients, generates more installation costs. Hence, we suggest the following proposition regarding installation cost within artificial costs.

**Proposition 5:** The higher installation cost recognizes by the businesses, the lower intention to switch to a new CAV.

## Conclusion

The conceptual model of this paper is based on three types of switching costs. These distinct types of switching costs will individually or collectively influence in switching CAV. Learning costs have the least influence on switching decisions, transaction costs and artificial costs have a significant effect on switching decisions. Furthermore, the combination of these two costs makes switching decisions even more complicatedness.

Our study contributes to security research in several ways. First, based on the interview results, we constructed an index map to detail kinds of switching costs, as shown in Tables 7-1 and 7-2. The index maps can help businesses identify which type of switching costs affect them most, and can assist them when evaluating various CAV packages. If there are more "Yes" than "No" answers, it means that the switching costs are lower. Conversely, more "No" than "Yes" answers implies that the switching costs are higher.

**Table7-1: An index map for evaluating CAV switching costs**

| Type | Assessment | | |
|---|---|---|---|
| Transaction Costs | Bounded Rationality | Yes | No |
| | Customers evaluate all CAV packages on the market | | |
| | Opportunism | Yes | No |
| | Customers trust provider's (or certificated reseller's) reputation. | | |
| | Customers believe the information that provider (or reseller) provide | | |
| | Assets specificity | Yes | No |
| | No need to buy extra hardware when switching to new CAV | | |
| | Excepting new CAV, no need to buy extra software when switching to new CAV | | |
| | No need for long-term training when switching to another CAV | | |
| | Uncertainty | Yes | No |
| | Pretest the new antivirus software before switching | | |
| | Changing the CAV will not affect the company's existing IT structure | | |
| | Transaction costs | Low | high |

**Table7-2: An index map for evaluating CAV switching costs**

| Type | Assessment | | |
|---|---|---|---|
| Artificial Costs | Existing provider | Yes | No |
| | The provider offers discounts in order to sell CAV | | |
| | The provider offers free training for CAV | | |
| | Substitute provider | Yes | No |
| | The provider offers a price discount to attract the potential buyer | | |
| | The provider offers free training for the new CAV | | |
| | The provider offers free installation of CAV in all clients (included in the purchase price) | | |
| | Artificial costs | Low | High |

Second, CISO is unable to measure the performance and effectiveness of various CAV precisely due to the lack of deep domain knowledge and bounded rationality. Because of these limitations, businesses prefer to adopt CAV from industrial leaders, rather than second-tier providers. Therefore, providers' market share and brand reputation are important while businesses adoption about CAV. Third, the adoption cost plays a vital factor in the decision-making process of switching CAV. That means when businesses evaluate the CAV among Symantec, Trend Micro, and McAfee; a provider who offers the lowest price could be the winner. Thus, our research suggests that second-tier providers use "low-price" as a strategy to attract customers who normally purchase CAV from industrial leaders. Nevertheless, brand reputation is still very important for second-tier providers in the antivirus industry, so they must prove that their software performances are better than the industrial leaders.

Finally, as mentioned earlier, after-sales service is important in the antivirus industry, providers should be responsible for helping businesses solve virus outbreak. However, it is evident that businesses need more assistance in the areas of controlling virus outbreak. This research found that businesses always fight their own 'virus wars' without assistance from their providers. Hence, we suggest that providers should be more proactive in helping their customers by providing security solutions that meet the customers' needs. This would increase a customer's artificial costs and lock-in the customer further.

Though this study provides a lot of insights to the CAV switching decision, it has several limitations. The study used the case study methodology and thus was limited by the sample size of the four companies that we used to collected data from, and hence is limited by the application of the finding. Studying the information security issue from the managerial perspective is a new concept. It will be helpful to understand the different aspects of the CAV switching decision by observing and interviewing more cases.

While this study has its limitation in generalizing the findings across different business settings, the insights gained in this study can still be of value to some businesses situations. More knowledge may be added to this subject through accumulating more case examples. In addition, the decision about switching CAV is not solely based on the switching costs and the software's effectiveness. Except these factors, there may be other factors that influence the corporate antivirus software switching decision, e.g. a business's political power, and are worthy of further study.

## References

Burke, B. et al. "Worldwide Antivirus Software Market Forecast and Analysis 2001-2005," *Internet Data Center Report*, 2004.

Chen, P.Y. and Hitt, L.M. "Measuring Switching Costs and the Determinants of Customer Retention in Internet-Enabled Businesses: A Study of the Online Brokerage Industry," *Information Systems Research* (13:3), 2002, pp. 255-274.

Coase, R. H. "The nature of firm," *Economica*, N.S.4, 1937, pp. 386-405.

Eisenhardt, K. M. "Building Theories from Case Study Research," *Academy of Management Review*, (14:4), 1989, pp. 532-550.

Fornell, C. A. "A National Customer Satisfaction Barometer: The Swedish Experience," *Journal of Marketing* (56:1), 1992, pp. 6-21.

Gordon et al. "CSI/FBI Computer Crime and Security Survey," *Computer Security Institution Annual Survey*, 2005.

Hsieh, H. M. "A Study on Growth Strategy of Antivirus Software Providers," *Master thesis of National Taiwan University*, 2003.

Hsieh, Y. C. et al. "Virtual Factory and Relationship Marketing-A Case Study of a Taiwan Semiconductor Manufacturing Company," *International Journal of Information Management* (22:2), 2002, pp. 109-126.

Hubbard, J.C. and Forcht, K.A. "Computer Viruses: How Companies Can Protect Their Systems," *Industrial Management & Data Systems* (1), 1998, pp. 12-16.

Kaspersky, E. "The Contemporary Antivirus Industry and Its Problems," Nov 2005 (available online at http://www.viruslist.com/en/analysis).

Keller, S. and Powell, A., et al. "Information Security Threats and Practices in Small Businesses," *Information System Management* (22:2), 2005, pp. 7-19.

Khalfan, A. "Information Security Considerations in IS/IT Outsourcing Project: A Descriptive Case Study of Two Sectors", *International Journal of Information Management* (24), 2004, pp.29-42.

Kim M., et al. "Estimating switching costs: the case of banking," *Journal of Financial Intermediation* (12:1), 2003, pp. 25-56.

Kim, G., et al. "A Study of Factors that Affect User Intentions Toward Email Service Switching," *Information& Management* (43), 2006, pp. 884-893.

Klemperer, P. "Competition When Consumers Have Switching Costs: An Overview With Application to Industrial Business, Macroeconomics, and International Trade," *Review of Economic Studies* (62:2), 1995, pp. 515-539.

Klemperer, P. "Market with Consumer Switching Costs," *The Quarterly Journal of Economics* (102:2), 1987, pp. 375-394.

Kotulic, A. & Clark, J. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), 2004, pp. 597-607.

Laudon, K. C., et al. *Management Information Systems*, Pearson Education, 2000, p. 97.

Liu, Y. C. "An Evaluation on Antivirus Software Performance," *Master thesis of Central Police University,* Taiwan, 2003.

Mamaghani, F. "Evaluation and Selection of An Antivirus and Content Filtering Software," *Information system & computer security* (10:1), 2002, pp. 28-32.

O'Brien, J. A. *Management Information Systems*, McGraw-Hill Publication, 2004, pp. 44-45.

Porter, M. E. "Strategy and the Internet," *Harvard Business Review* (79:3), 2001, pp. 62-78.

Post, G. and Kagan, A. "Management Tradeoffs in Anti-virus Strategies," *Information & Management* (37:1), 2000, pp. 13-24.

Potter, C. and Beard, A. "Information Security Breaches Survey 2006," *Department of Trade and Industry Annual Report*, 2006 (available online at http://www.pwc.com)

Robbins, A. "The Virus Wars." *PC Magazine*, July 6, 2004, p. 114.

Roberts, P. "The Cost of Virus Protection Rises," *PC World* (23:1), Jan 2005, p. 24.

Wang, E. T. G. "Transaction Attributes and Software Outsourcing Success: An Empirical Investigation of Transaction Cost Theory," *Information System Journal* (12:2), 2002, pp. 153-181.

White, G. and Pearson, S. "Controlling Corporate e-mail, PC Use and Computer Security," *Information system & computer security* (9:2), 2001, pp. 88-92.

Williamson, O. E. "The Economics of Organization: The Transaction Cost Approach," *The American Journal Sociology* (87:3), 1981, pp. 548-577.

Williamson, O. E. *The Economic Institutions of Capitalism*, The Free Press, New York, 1985.

Yin, R.K. *Case study research: Design and Method*, Sage Publication, 1994.