Innovation as Guided Coevolution:
The Trend Micro Case (1998 – 2005)

Anthony Kuo[1], Shih-tse Lo[2], Dhanoos Sutthiphisal[3], and Ivy Chiu

[1] PhD Program, College of Management, Fu Jen Catholic University

[2] Martin de Tours School of Management and Economics, Assumption University

[3] Martin de Tours School of Management and Economics, Assumption University

[4] PhD Program, College of Management, Fu Jen Catholic University

shihtselo@msme.au.edu

Abstract

Innovation is considered crucial for firms to compete effectively. The extant research on innovation has provided significant insights, but, however, the majority examined innovation in the context of technology. Only a few exceptions have explored how social and behavioral factors influence firms in the innovation processes. Based on the coevolution perspective, this study examines innovation process of a software firm participating in the ever-changing information security software industry. We focused on how the firm guided its offerings to coevolve with new technologies and relevant changes among different groups of human actors. Our data reveals that the firm developed different offerings in different periods to cope with the changing driving forces—technologies, users, and hackers—in each period. Effectively identifying the driving forces and guided its offerings to coevolve with them, the firm successfully sustained its competitive advantage in the period characterized with turbulence in the environment.

Keywords: innovation, coevolution, software, high-tech

JEL : O36

DOI : 10.24002/kinerja.v22i2.3227

Received : 09/28/2019 Reviewed: 10/29/2019 Final Version: 29/01/2020

1. INTRODUCTION

It is doubtless that widely accepted that innovation plays a crucial role in a firm's competitiveness (e.g. Hitt 1999; Ireland and Hitt 1999; Hamel 2000). Researchers in various disciplines such as organization, marketing, engineering and new product development have conducted numerous studies on the origin, forms, types, and processes of innovation, providing fruitful insights to advance our knowledge of innovation. However, far more attention has been paid to technologies than to human and social aspects, the factors yet to be fully tapped by innovation scholars (e.g. MacKenzie and Wajcman 1985; Williams and Edge 1999).

In this paper we aim to contribute to a better understanding of how technologies and human actors interact to drive the changes, and how a firm identifies the driving forces of changes and take managerial actions to coevolve with the changes. We conduct a single historical case study to examine the innovation process of a software firm in a turbulent high-tech industry characterized by frequent and rapid changes of technologies and relevant human actors. Evidence from our case study indicates that the firm effectively identified the driving forces in the environment and guided its offerings to coevolve with new technologies and relevant social changes. The firm successfully sustained its competitiveness via such a process of guided coevolution, and, in turn, created new market segments to re-shape industry.

The current study contributes to the existing literature in several ways. First, it provides insights to enrich the theory of innovation process by integrating and synthesizing technological aspects and human actors in the theory of innovation process. Second, this study contribute to the study of coevolution of organizations and their environments (Lewin and Volberda 1999). Third, this paper provides insights for high-tech companies to take consideration of both technologies and human actors in their innovation process.

2. LITERATURE REVIEW

The majority of innovation studies have been focusing on technology. For example, innovations are distinguished as incremental (continuous) or radical (discontinuous). An incremental innovation exploits existing technologies, improves current designs, and introduces minor changes to products or services. Radical or discontinuous innovation, in contrast, is based on technological breakthroughs and often create opportunities for new applications and new markets (Ettlie et al. 1984; Dewar and Dutton 1986; Tushman and Anderson 1986). This stream of research on technological innovation was further extended and refined to include notions such as "architecture innovation" (Henderson and Clark 1990), which is based on linkages between core concepts and components; and "disruptive innovation"

(Christensen 1997), which identified the possibility that technologies with inferior performance can displace established incumbents.

The above innovation researches have produced important insights. However, focusing solely on technology also brought limitations. The influence of other factors has yet been fully explored, except for psychological variables such as 'perceived usefulness' and 'perceived ease of use' in the innovativeness adoption model (Rogers 1995) or technology acceptance model (Davis 1986; Podolny and Stuart 1995; Venkatesh and Davis 2000). Even these models take psychological factors into account, they consider technology the driving force of innovation, emphasizing how organizations can conduct internal activities to "adopt" or "accept" emerging technologies in their external environments.

To augment the insufficiency of the above "technology-economic paradigm", another stream of technological innovation research—the tradition of social shaping of technology (MacKenzie and Wajcman 1985; Williams and Edge 1999) —endeavored to incorporate social factors in the process of technological advancements. This stream of studies has shed light on how social forces influence progress of technological innovation, but has paid little attention to an organization's internal efforts on innovation and the possibility that a firm's innovation can, in turn, shape the development of technology. Therefore, a holistic approach that takes technological, social, and managerial factors into consideration will help us to better understand how a firm can innovate to remain competitive in an environment with changing technologies.

To examine the joint effects of technological, social, and managerial factors in the innovation process, we believe the coevolution perspective is appropriate because "the coevolution lens has the potential for integrating micro- and macro-level evolution within a unifying framework, incorporating multiple levels of analyses and contingent effects, and "leading to new insights and new understanding" (Lewin and Volberda 1999). We follow Lewin and Volberda's perspective that "change may occur in all interacting populations of organizations", and use their definition of coevolution as "the joint outcome of managerial intentionality, environment, and institutional effects" (Lewin and Volberda 1999). Such a perspective is not suitable for the use of quantitative methodologies. Thus, we adopt the qualitative approach as our research methodology.

3. METHODOLOGY

Several reasons explain why the qualitative approach is more adequate. First, when organizational processes such as innovation processes are involved, quantitative measurements are inappropriate (e.g. Van Maanen 1979; Strauss and Corbin 1990), as are survey-based methodologies (Yin, 1983). Second, the coevolutionary perspective, which incorporates multiple levels of analyses to investigate the joint outcome of managerial actions and environmental effects, calls

for a fine-grained process study (Lewin and Volberda 1999). Such a process study can only be explored thoroughly via qualitative approaches such as in-depth case studies (e.g. Yin 1983; Strauss and Corbin 1990). Therefore, in this paper, we use a single case study for the purpose of elaborating upon a set of intertwined multilevel relationships and concepts necessary for process theory development. The objective of the case analysis is to investigate the coevolution of relevant human actors with technologies, as well as how a firm identifies the driving force in the ecosystem and then purposefully guides its offerings to coevolve with them.

We chose this particular industry context—the antivirus and information security software industry—for two reasons. First, the antivirus and information security software industry are characterized with turbulent changes, in both technologies and human actors, and in both industry macroevolution and firm microevolution as well. Technological and human actors, such as users and hackers, are inextricably intertwined, and thus provide an ideal setting for innovation process study in the coevolutionary perspective. Second, the case company, Trend Micro Inc., is highly recognized by industry analysts, such as IDC, for its innovativeness (Burke 2004). Examination of its innovation process will bring significant insights. The time frame of 1998 to 2005 was chosen because in this period, the antivirus and Internet security saw the biggest changes, compared to those in other periods.

In the following section, we will first introduce the industry background by explaining how computer viruses have evolved and related how human actors, including users and hackers, have involved. Then we describe the stages of the coevolution process, elaborating how the case company purposefully guided its offerings to coevolve with three relevant populations: technologies, hackers, and users.

4. INDUSTRY BACKGROUND

4.1. Computer viruses and malware

A computer virus is a program—usually a piece of executable code—that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They attach themselves to just about any types of files and proliferate by residing in files that are copied and sent from individual to individual. In addition to replication, a number of computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat the hard drive, or cause other damage. If the virus does not contain a damage routine, it can cause problems by consuming storage space and memory, degrading the overall performance of the computer, or consuming precious network bandwidth, bringing tremendous troubles and interruptions to computer users both at home and in business operations.

Not every piece of code that interferes with the proper functioning of computers is a virus. In fact, the broader term generally used in the industry is “malware” (sometimes called malicious software or malicious code). Malware is a typology that includes not only viruses but also other code or software contaminants. Although a virus may be distinguished from other types of malicious code (for example, a worm or a Trojan horse), it remains the most generally understood and frequently used term to encompass all of these malicious programs. In this study we do not distinguish viruses from other types of malware. The main reason is that we intend to avoid unnecessary confusion, because the convergence of different types of malware has been observed and has kept blurring boundaries among them. We use the terms “viruses”, “malicious codes”, or “malware” interchangeably to represent all types of malicious programs that are detrimental to computer usage.

4.2. Technologies, users, and hackers

The virus-fueled multifaceted changes in threats that complicated the information security software industry were actually a joint outcome caused by continuous coevolution of technologies and human actors such as hackers and users. Changes only in technologies could hardly have led to such upheavals.

Users play a crucial role in the information security industry. In this study, we refer to users as individuals, organizations, or other entities that employ the resources or services provided by a computer system. The needs of users shape technological development—and in turn, behaviors of users are affected by technologies. The word “hacker” was originally used in the computing community to describe a particularly brilliant programmer or technical expert. Today it generally describes computer intruders or criminals. Some people advocate terms such as "cracker" or "black-hat" to replace it; others prefer to retain the common popular usage, arguing that the original form is confusing and will never likely be pervasive. In this study, we follow the common popular usage of the term “hacker” to include different sorts of malicious computer professionals who sabotage computer security. These people include virus writers, intruders, crackers, vandals, etc. Hackers exploit new technologies to undertake hacking activities: their tools have been increasingly sophisticated as new technologies developed, and they always utilize the most advanced and prevalent technologies to create havoc. Their motives and intentions have also evolved over time.

Analyzing the data obtained, we find that the driving forces of coevolution are different in different periods of time. Technologies, users, and hackers—the three highly intertwined populations in the ecosystem—take turns to drive the coevolution process. Each population exerts influences on the other two and shape their development. Our case company recognized the phenomenon, and purposefully guided its internal innovation activities to coevolve with the three elements.

5. CASE DESCRIPTION AND RESEARCH FINDINGS

Our case company, Trend Micro Incorporated, produces antivirus and Internet content security software products and services. Its solutions protect the flow of information on PCs, file servers, email servers and at the Internet gateway, providing comprehensive and centrally controlled management for enterprise network security. Founded in 1988, the Tokyo-based corporation was the fourth largest secure content and threat management software company in the world in 2007 (Burke et al 2007), employing more than 3700 people in 30 countries. Sales have soared by an average of nearly 75% per year over the past decade, reaching US$848 million in 2007. The company has been listed on the Tokyo Stock Exchange (4704) since 1998, and was chosen as a component of the Nikkei Stock Average on September 19, 2002. The 225-share Nikkei Stock Average is Japan's most widely followed stock market index, composed of leading companies listed on the First Section of the Tokyo Stock Exchange.

Examining Trend Micro's history of innovation, we found evidence that the company has been purposefully guiding its new offerings, including products and services, to coevolve with technologies, hackers, and users. In different periods of time, different populations drove the coevolution process. The company recognized signs of changes and seized opportunities to initiate innovations.

5.1. Stage 1 (1988 – 1994)

5.1.1. Technologies drove the coevolution in Stage 1 (1988 – 1994)

Coevolution in this period of time was mainly driven by technologies. Technologies relevant to viruses include programming languages and platforms, and hackers have been continually exploiting advances in these technologies to compose viruses. Programming languages is a standardized communication technique for expressing instructions to a computer. It is the basis on which viruses and other malicious codes are composed—just like different toxicants are created based on different chemical elements. As time went by, new programming languages emerged, and thus provided new bases for hackers to create new types of viruses.

Viruses first appeared on personal computers in the 1980s, when Microsoft DOS was the most prevalent platform of PCs. Platforms have always played a dominant role in the history of PCs, providing a basis on which different applications are built. Dominant platforms on PCs evolved from DOS to Window 3.x and then to Windows 95 in this period of time; hackers consequently created new species of viruses to infect these different platforms.

On the other hand, advances in technologies also changed users' perceptions and behaviors. Traditionally, virus infection was perceived as a problem on personal computers, and it was the individual user's responsibility to protect his or her own PC, either at home or in the office. Most users installed antivirus software on their own PCs to scan for viruses, and endeavored to remove viruses and

recover the computer by themselves whenever a virus was found. This practice did not change until the rise of local area networks (LANs).

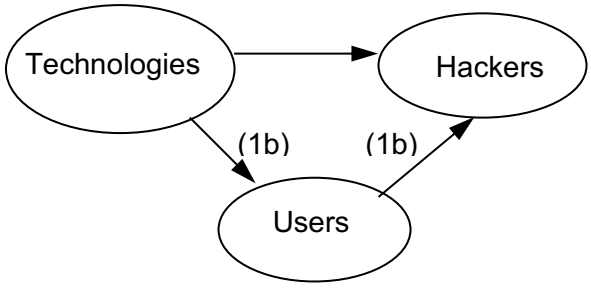
In the late 1980s and early 1990s, LAN technologies were swiftly developed and grew to be ubiquitous. Novell NetWare dominated the LAN market with nearly 70% of market share. Before LAN, users exchanged files by swapping floppy diskettes with each other. The prevalence of LAN enabled users to exchange information via the network. More and more people stored files on "servers," computer systems that shared them with other computers upon users' requests. Exchange of files among users thus became faster and easier. Gradually the servers became very important "storage rooms" and "file exchange centers" for most users.

Development of LAN technologies changed users' information-sharing behavior and facilitated information exchange. Unfortunately, it also created a new path for viruses to spread. Before LAN was available, viruses travel via floppy diskettes when a user saved his or her files on the diskette and passed it to somebody else. But when users shared files via LAN servers, an infected file stored on the server could be accessed by many users simultaneously and thus infect all their computers.

In the period between 1993 and 1994, commercialization caused the Internet to develop rapidly and grow explosively. Once again, new technology enabled users to explore new ways of information-sharing. Email, FTP (file transferring protocol), and WWW (world wide web) quickly became the most prevalent applications on the Internet (Moschovitis et al 1999). People downloaded files from web sites and utilized FTP sites to obtain and send files as they did with servers in the era of LAN. They also attached files to emails and sent to their family, friends, colleagues, and business associates. This again created a new means for viruses to spread. However, viruses did not spread via the Internet in this period of time. Rather, the major Internet virus outbreaks happed in Stage 2 (1995 – 2000) we specified in this study. We will elaborate upon this later.

Overall, in the period between 1988 and 1994, technologies drove the coevolution. First, technological advances, including new programming languages and new platforms such as Windows for PCs, enabled hackers to exploit new techniques to write viruses. Meanwhile, LAN and Internet technologies also allowed users to share information via networks, thus creating new means for virus infections. Figure 1 illustrates how technologies drove the coevolution in Stage 1 (1988 – 1994).

(1a)



(1a) Technological advances enabled hackers to exploit new techniques to write viruses.
(1b) LAN technologies changed users' information sharing behavior to replace floppy diskettes with networks to share information, and thus created a new means for viruses to spread (via networks).

Figure 1. Technologies drove the coevolution in Stage 1 (1988 – 1994)

5.1.2. Trend Micro's guided coevolution of new offerings with technologies and other populations (1988 – 1994)

Trend Micro's executive recognized the influence of new technologies and the coevolution process, and consequently developed different antivirus software programs so that different platforms could coevolve. As new programming languages and new PC platforms developed, Trend Micro's engineers developed software products accordingly. The company's PC-based antivirus software "PC-cillin" was first developed on MS-DOS, and later "ported" (transferred to a new platform by using new programming techniques) to the Windows platforms.

As LAN technologies developed and prevailed, Trend Micro's executives realized that servers could turn into "virus exchange centers" and consequently alerted users of the dangers. At that time, however, no protection mechanisms were available on the servers. The company's engineering team began to develop the first antivirus software in the world, running on Novell NetWare Servers. The prototype was completed in 1991 and named "LANProtect." It was later changed to "LANDesk VirusProtect" when the program was licensed to Intel. The product was launched in 1992 as part of Intel's network management software, LANDesk Management Suite, and distributed in the market until 1998. Trend Micro Inc. ended the OEM relationship with Intel in 1998 and launched its own version of server-based antivirus software, ServerProtect. The product was further developed to run on Microsoft Windows NT Server when Novel NetWare gave way to Windows NT.

The server-based antivirus software was a breakthrough in the antivirus industry. At first there was no competition in the market, but similar products proliferated quickly. Since 1993, there have been seven vendors offering LAN server-based antivirus software in the market (Mark 1993). Server-based antivirus software gradually gained popularity among users. In 1997, five years after the initial launch, the server-based antivirus adoption rate has reached 54% (ICSA 2005). Server-based antivirus software later became de facto in antivirus software product mixes. Today, virtually all antivirus software vendors produce and market similar products. In 2003, the server antivirus market reached $222 million, led by Trend Micro with a 26.3% market share (Burke 2004). The server-based antivirus adoption rate in 2004 reached 95% (ICSA 2005). These statistics reveal the profound influences of Trend Micro's early innovations on the antivirus industry as

a whole. Virus protection was no longer merely an issue on desktop PCs; users ultimately perceived it as a network security issue.

As Internet developed and commercialized rapidly, Trend Micro again saw the behavioral changes of users. It foresaw the possibilities that viruses might travel through email attachments and file downloads on the Internet, and thus spread to organizations' internal networks. Hence, it started to develop antivirus software at the Internet gateway, where the internal network of an organization is separated from external networks (i.e. the Internet). The product, InterScan VirusWall, was launched in 1995. In the following section, we will provide more details of the product launch and its consequences.

5.2. Stage 2 (1995 – 2000)

5.2.1. Users drove the coevolution in Stage 2 (1995 – 2000)

Coevolution in this period of time was primarily driven by users. Adoptions and development of corporate networks skyrocketed. Numerous organizations built up networks to connect their remote offices with their headquarters. As the Internet retained its astonishing penetration rate in this period of time, users soon relied heavily on email to share information and conduct business.

The surge of users' reliance on email encouraged major software vendors such as Lotus (later a division of IBM) and Microsoft to develop their proprietary software of email systems, which soon gained popularity among corporations. A significant number of corporations adopted Lotus Notes Server or Microsoft Exchange Server as their email systems, either connected to the Internet or for internal communications only. Lotus and Microsoft further expanded functionalities of Notes and Exchange, respectively, to facilitate collaboration among users in the same organization. They repositioned their products to "groupware", which is software designed to help people involving in a common task. This new type of software further attracted more users. Lotus Notes accumulated 17 million installations from 1989 to 1998, while Microsoft Exchange gained 9.5 million from 1996 to 1998 (Lyons 1998).

Adoptions of groupware enhanced communications and collaboration among users (Brennan and Rubenstein 1995). Email soon replaced floppy diskettes as a main medium for file exchange. However, the prevalence of email also motivated hackers to explore new ways of virus composition and distribution. As stated earlier, hackers intended to cause havoc, so they kept exploiting the most popular means of information-sharing to write and spread viruses. In the mid- 1990s, lots of users used Microsoft Word to create documents and share with each other via email attachment, so Microsoft Word and email became the most prominent targets for viruses.

The 1996 advent of "Concept", the first Word Macro virus (composed with Microsoft Word Macro commands) signals a paradigm shift in computer viruses. It resided in Microsoft Word documents, not in executable program files as traditional viruses did. When a contaminated copy of a Word file was opened, the virus

infected new Word files created afterward. Soon the new virus spread, and new Word Micro viruses with similar infecting schemes proliferated. Exacerbated by intensive use of email to exchange Word files, Word Macro viruses propagated exponentially, and quickly became the most prevalent species in 1996 and 1997 (ICSA 1997).

Users' increasing adoption of email, together with prevalence of the Word Macro viruses, rapidly changed the landscape of virus infection methods. The radical change reached its apex in 1999 when "Melissa", the first email-borne virus, broke out. The Melissa virus hit corporate sites on March 26, 1999 (later known as the M-day). This Word macro virus had the unusual characteristic (at the time) of attaching itself in the email to spread. Whenever a victim opened the infected Word document in his/her email, the virus immediately invoked composition of a new email, attaching itself in that email and then being forwarded to people listed in the victim's address book. Soon the Melissa virus swept throughout corporate networks, leading to a catastrophe. According to the estimation of ICSA (1999), 482,869 PCs were exposed to the risk of Melissa within a week after the outbreak, and the average infection rate for each Melissa incident reached approximately 76 per 1,000 PCs (ICSA 1999). In addition, Melissa was found to be "more than 38 times more frequent as the cause of virus disasters in the 30 companies who experienced virus disasters after M-day" (ICSA 1999).

The outbreak of the Melissa virus signified the arrival of the era of email-borne viruses. In 1999, email attachments replaced floppy diskettes as the most important means of infections. In the subsequent years, similar viruses such as "ILOVEYOU" and "AnnaKournikova" broke out time and again, causing tremendous losses for users. Table 1 shows the statistics on sources of virus infections from 1996 to 2000. We can easily observe that, from 1996 to 2000, viruses spreading via email surged, while floppy diskettes gradually disappeared from the list of major means of virus infection.

Table 1. Sources of virus infections, 1996-2000

Virus source	1996	1997	1998	1999	2000
Email Attachments	9%	26%	32%	56%	87%
Diskettes	71%	84%	64%	27%	7%

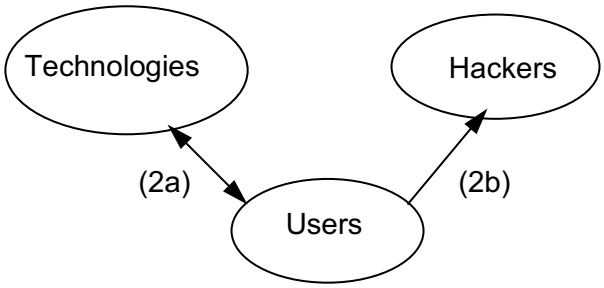
Source: ICSA Labs Virus Prevalence Survey 2004

As users increasingly relied on email and networks for daily operations, the growing complexity and scattered pieces of software on the networks made it very difficult to manage and update antivirus software so it could catch the latest viruses. This called for a centralized management scheme. For computer network managers in an organization, keeping track of all the antivirus software scattered throughout the network constituted a chronic headache, especially when an

organization had branches located in multiple geographical regions. The need for a centralized management of antivirus software on the network soon became crucial.

To summarize, in the period between 1996 and 2000, users drove the coevolution. First, users' adoptions of networks and email encouraged software firms to develop new related software, such as Lotus Notes and Microsoft Exchange. This in turn facilitates users' reliance on email to share information. In addition, complexity of networks increased dramatically in this period, and thus created the need for centralized management of antivirus software on a network. Meanwhile, users' heavy reliance on email motivated hackers to write viruses that can wreak spreading havoc via email and networks.

Figure 2 illustrates how users drove the coevolution in the period from 1995 to 2000. Note that some of the influences of users on technologies are bi-directional. In this stage, users' adoptions of email and networks stimulated developments of related software, such as Lotus Notes and Microsoft Exchange. The new email software, in turn, attracted even more users to rely on email to communicate. The phenomenon of circular causality is observed in the mutual influences between users and technologies.



(2a) Users' adoptions of email and networks spurred development of more email and groupware software, such as Lotus Notes and Microsoft Exchange, which in turn facilitates users' reliance on email and groupware software. Complexity of network increased dramatically and thus created users' needs for centralized management for antivirus software.
(2b) Users' reliance on email motivated hackers to write viruses to spread via email and networks to cause havoc.

Figure 2. Users drove the coevolution in Stage 2 (1995 – 2000)

5.2.2. Trend Micro's guided coevolution of new offerings with users and other populations (1995 – 2000)

During this period of time, Trend Micro endeavored to guide its new product offerings to coevolve with the user-driven coevolution. In response to the increasing use of the Internet and email to share information, Trend Micro's product team started the development of its Internet gateway antivirus software in 1994. The product, InterScan VirusWall, was finally born in 1995, and became the first Internet gateway antivirus software in the world. Similar products were shipped

by two major competitors, McAfee and Symantec, until June 1996 (Vance 1996) and February 1997, respectively.

The LAN server antivirus took five years to reach a penetration rate of 54%. Internet gateway antivirus programs gained users' acceptance at an even faster pace. In 1999, four years after Trend Micro's InterScan VirusWall was launched, adoption rate of Internet email gateway antivirus software reached 53% (ICSA 2005). The VirusWall was eventually patented and further facilitated the company's fast growth. Statistics showed that the adoption rate of Internet email gateway antivirus programs amounted to 80% in 2000 and 84% in 2001 respectively (ICSA 2005). With the first-mover advantage, Trend Micro led this market segment for several years. This segment grew to US$ 338 million in 2003, with a 35.7% market share taken by Trend Micro (Burke 2004). Gateway based antivirus systems later became ubiquitous—96% of organizations by 2004 had adopted antivirus protections for their email gateways (ICSA 2005).

In addition, Trend Micro also started to develop virus scanning products for proprietary email systems. The software is meant to stop the viruses before they get delivered to numerous end users, much like checking for anthrax in mail at post offices. These two products were launched in 1996 and 1997 respectively, but demand remained weak because of a general lack of awareness of potential damages caused by email viruses. Trend Micro's product team developed the email-based antivirus software mainly because it did have an awareness, as per interviews with Trend Micro managers.

But in 1999, when the first email-borne virus "Melissa" broke out, the two products proved their worth. During the outbreaks, the software successfully blocked tons of copies of the Melissa virus on email servers, inhibiting it from spreading to email recipients. Consequently, Trend Micro's competitors announced similar products after the company launched its ScanMail products. Email-based antivirus software developed by these firms together later created a new market segment in the antivirus industry, with Trend Micro leading the segment worth a total of US$ 328 million in 2003 by a 20.1% market share (Burke 2004).

Innovations in email-based antivirus software also changed users' perceptions and behaviors regarding antivirus programs. An increasing number of users started to regularly scan email traffic in real time for viruses, and certain file attachments were blocked, filtered, or quarantined on the email servers to reduce chance of infection. Within a few years, virtually all users who have adopted email antivirus software have set certain email policies. Statistics shows that, in 2004, 99% of these users scan their email traffic in real time, 93% of them block, filter, or quarantine email attachment by file types, and 70% of them scan message folders or databases (ICSA 2005).

Trend Micro once again guided its product offerings to coevolve with users. The company's product team utilized the burgeoning field of web-based programming technologies and systems technologies to create the "Trend Micro

Control Manager", a software tool that centrally controls and manages all the antivirus software on an organization's network. The company even changed its corporate slogan to "central control is the only virus control" for a certain period of time.

The product was initially launched 1998, the same year the company filed its IPO. This management utility solved many corporate IT headaches regarding antivirus software. Such a utility has later become the de facto standard in antivirus software, with most antivirus software companies offering similar tools.

5.3. Stage 3 (2001 – 2005)

5.3.1. Hackers drove the coevolution in Stage 3 (2001 – 2005)

In this period of time, hackers gradually took their turn to drive the coevolution. Since the first email-borne virus "Melissa" burst onto the scene in 1999, viruses became ever more complicated, with lots of new types created using different techniques. The peak arrived in 2001 when the hybrid types of viruses broke out. Why did such an upheaval take place? We attribute it to changes in hackers' community.

Two prominent trends were observed in hackers' community: integrated security breaches and change in hackers' motives and intentions. First, various hacking techniques started to converge in this period, mainly due to an abundance of hacking resources on the Internet. Traditionally, hackers were either programming experts or savvy systems engineers who possessed high proficiency in computer engineering. However, as networking technologies matured, hackers exploited them by posting tools and guidebooks on the Internet to share with each other. Any ill-intended computer amateur could easily download these tools and become hackers (Boulanger 1998). The wide availability of these resources enabled all the "bad guys"—such as vandals, crackers, spammers (people who distribute unsolicited email), and virus writers—to adopt each other's techniques to perpetrate. Key examples included the high-profile DDoS (distributed denial-of-service) attacks targeting famous web sites like Yahoo, CNN, and Amazon, and assaults aimed at the White House web site during the outbreak of the Code Red worm in 2001. Hackers used tools such as Code Red, Trinoo, TFN2K, or Shaft to plant malicious codes on innocent computers (called "zombies") on the Internet, and took advantage of the zombies to launch attacks. This was a brand new technique, because previous security breaches had never involved such sophisticated tools and schemes.

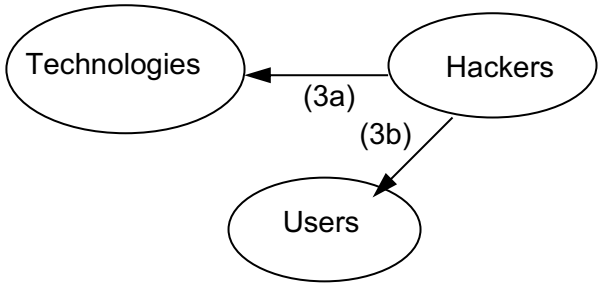
Second, motives and intentions of hackers changed in this period. In the past, viruses and other malicious codes were typically composed for fun, or to create chaos to seek notoriety. However, in more recent years, hackers have been increasingly motivated by financial gains. They use malware to commit organized crimes such as obtaining credit card numbers, stealing bank account information, exploiting other personal information, or threatening to publish the victim's data or perpetually block access to it unless a ransom is paid. As a consequence, online

frauds and identity thefts proliferated after 2001, with increasing sophistication and scale (Burke 2004).

The new wave of hybrid types of computer viruses such as Nimda and Code Red finally blasted through the Internet in 2001, presenting an unprecedented challenge for IT staff in organizations (ICSA 2002). These were not totally new types of viruses. Instead, they were a hybrid of several existing techniques, including viruses, worms, and hackers' tools. Email attachments were no longer the only media by which they spread; they acted like hackers, spread like spam (unsolicited commercial email), and destroyed data on computer systems in organizations. They exploited flaws in Microsoft and other firm's software to compromise targeted machines. To a certain extent, the hybrid malware obsolete existing security solutions, such as antivirus software, firewall systems and intrusion detection system, because no single solution could effectively stop the new attacks.

Most users were baffled and frustrated in trying to stop the hybrid digital vermin. In subsequent years, the rapidity, frequency and complexity of spreading infections continued to increase as organizations relied more and more on the Internet for business operations. Network unavailability caused by virus or worm attacks became ever more intolerable for organizations. However, since no single existing security product could effectively stop the attacks, users could merely disconnect the network temporarily whenever a hybrid malware broke out, and wait for the storm to end (Richardson 2003). If viruses still sneaked into the internal network, nothing could be done except to clean up the remnants and then try to restore the computer systems as soon as possible. This usually cost significant time and efforts.

We use Figure 3 below to summarize how hackers drove the coevolution from 2001 to 2005. Basically, hackers (including vandals, crackers, spammers, and virus writers) started to exploit each other's techniques. Together with changes in hackers' motives and intentions, existing products could no longer protect users from attacks, rendering them bewildered and helpless.



(3a) Convergence of hacking techniques, along with changes of hackers' motives and intentions, made extant protecting technologies obsolete.
(3b) Users were baffled, but could not find any effective solutions to stop new hybrid attacks.

Figure 3. Hackers drove the coevolution in Stage 3 (2001 – 2005)

5.3.2. Trend Micro's guided coevolution of new offerings with hackers and other populations (2001 – 2005)

Perceiving the severity of the new hybrid type of viruses, Trend Micro in 2001 conducted a comprehensive study. Officials visited over 300 organizations to investigate how users handled the hybrid virus problems. They found that companies typically dealt with the problem by installing antivirus and other security software or hardware, leaving other necessary policies, procedures and services unattended. Given the new environment, this approach had limitations, since it overlooked the big picture of the entire process. The reality was that security exploits were inevitable, because hackers would never stop attacking. The key was to design a strategy to mitigate damages caused by attacks, so normal business operations could continue without interruptions.

Based on these findings, Trend Micro designed a service offering named "Enterprise Protection Strategy." Launched in 2002, its aim was to deal with the problems from the perspective of threat lifecycle management. The service development team decomposed, analyzed, and restructured relevant procedures and processes, and designed the new services accordingly to help users handle security breaches.

The service has since evolved through different stages, expanding to cover more aspects of the entire process: planning, implementing, protecting, responding, recovering, monitoring, and auditing. New "Expert Services" covering a wider spectrum of security management was later developed and launched at the end of 2005.

5.4. Summary of Trend Micro's guided coevolution

The above analyses revealed how varying patterns of guided coevolution influenced new offerings due to hackers, users, and technologies in different time periods. A time line of Trend Micro's guided coevolution is provided in Table 2. Note that some of the effects of coevolution in the earlier stage were not obvious until the next stage. For example, the effects of technological advances in networks upon the first stage were not evident until users' increasing reliance on email was observed in the second stage. This "legging" phenomenon corresponds to researchers' calling for an analysis of historical data when conducting coevolution studies (Lewin and Volberda 1999). Without such analysis, we can never understand the coevolution process accurately.

Table 2. Time line of Trend Micro's guided coevolution

	Technologies	**Hackers**	**Users**	**Trend Micro's new offerings**	**Competitions**
Stage 1 (1988–1994)	• **MS-DOS , Windows, new programming languages, Local Area Network (LAN) developed and prevailed.** • **Novell NetWare dominated in the LAN operating systems.** • **Internet developed and started to commercialize rapidly.**	• Hackers adopted new technologies to write viruses to infect new platforms as Windows and LAN prevailed. • Viruses began to spread vastly through Windows and LAN respectively.	• Users switched from MS-DOS to Windows platform. • As LAN prevailed, users relied more and more on LAN, abandoning floppy diskettes, to share information. • Users started to adopt the Internet, especially via email, to share information.	• "PC-cillin" (PC antivirus software) for MS-DOS and for Windows platforms were launched as new platforms were brought to the world. • "LANDesk VirusProtect" (LAN based antivirus software) was launched in 1992.	• At first no rivalry existed in the market, but competition intensified very fast as competitors launched similar products. • Trend Micro has maintained its leading status in the LAN antivirus market segment.

	Technologies	**Hackers**	**Users**	**Trend Micro's new offerings**	**Competitions**
Stage 2 (1995–2000)	• Commercial use of the Internet grew swiftly. • Corporate networks developed. • Major software firms such as Microsoft and Lotus developed their software of email systems. • Web-based programming and systems technologies developed and were getting mature.	• Users' reliance on the Internet and email motivated hackers to exploit Internet to spread viruses. • The first Macro virus, "Concept", which infects Microsoft Word documents, was born in 1996, and Macro viruses soon began to spread vastly through the Internet. • The first email-blasting virus, "Melissa", broke out in 1999, and email soon became the most prevalent means of virus infections.	• **Users heavily relied on email to share information and conduct business.** • **Networks became inter-connected, and were thus getting very complex.** • **Users had difficulties to manage and update their antivirus software scattered on the network. Consequently, email viruses spread via the Internet explosively.**	• "InterScan VirusWall" (an Internet gateway antivirus software) was launched in 1995. • "ScanMail" for Microsoft Exchange and Lotus Notes email and groupware antivirus software) was launched in 1996 and 1997 respectively. • "Trend Virus Control System" (a centralized management utility for antivirus software) was launched in 1998.	• At first no rivalry existed in the market; competitors launched similar products soon after Trend Micro launched its innovative new software products. • As the first-mover in network-based antivirus software, Trend Micro kept leading this market segment.
Stage 3 (2001–2005)	• The hybrid types of viruses/worms obsolete existing security solutions, such as antivirus, firewall, and intrusion detections. None of these solutions alone could effectively stop the new hybrid attacks.	• **Convergence of hacking techniques took place.** • **Hackers changed their motives and intentions.** • **The new wave of hybrid types of computer viruses such as Nimda and Code Red blasted through the Internet in 2001.**	• Users were baffled when dealing with the new hybrid types of viruses. No effective solutions could be found to stop the new types of viruses.	• Trend Micro launched "Enterprise Protection Strategy" (an integrated threat lifecycle management service offering) in 2001. • Expert Services covering a wider scope was launched in the end of 2005.	• Competitors adopted different approaches to evolve. • More competition came from convergence of closely related species in the security industry.

Remarks: Shaded cells with bold fonts represent the driving force in the coevolution process.

6. DISCUSSIONS AND CONCLUSION

Several aspects of the findings in our case study may not be directly related to the theme of guided coevolution. However, they are worthy of more detailed discussions. We elaborate the details in the next section.

6.1. Identifying the driving force early may bring first-mover advantages

Trend Micro's experience provides a good managerial reference for high-tech firms regarding first-mover advantage. Our case study indicates that the company has maintained its leading position, for certain periods of time, in the market segments shaped by its innovations. As the research has revealed, it identified the driving forces early on in different stages of the coevolution process. After recognizing the driving force, the company proceeded to develop corresponding products or services, creating new market segments and raising entry barriers. Even though its competitors subsequently launched similar products, the company could still lead the market segment for a certain period of time and enjoyed the first-mover advantage.

6.2. Observing the social process of technological change to identify the driving force

Both technologies and relevant human actors, such as users and hackers, can drive the coevolution process. In our case study, technologies drove the coevolution in the first stage (1988–1994), as per the "technology-economic paradigm." But changes in human perceptions and behaviors sparked new opportunities for the case company to innovate in the second (1995–2000) and third stages (2001–2005). If users had never adopted network technologies and consequently changed their behavior to share information, or hackers had not kept exploiting new technologies to wreak havoc, viruses would still have been a PC security issue, and the information security industry landscape would be totally different. Therefore, it is critical for high-tech firm to pay additional attention to the behavior of human actors, along with technology development.

6.3. Limitations and future research suggestions

This study brings insights, but also has limitations. For example, we have only explored the role of two human actors—users and hackers—in the process of coevolution. The conceptual model drawn from the results is only applicable in the context of human-technology interaction, and the contribution of this study is therefore limited to the related context. More factors such as social, economic, institutional, cultural factors, etc. are also worth noting. We would like to call for more research to fill the gap.

We would like to propose some starting points. For scholars, the research by Dijksterhuis et al. (1999) may be a good reference on how to identify the source of coevolution when conducting academic research. In their paper, the authors explain how they identified the source of coevolution in new organizational forms. Although they intended to elaborate on how to design an organization to align with

its external environment, we believe their rationale will also help with identifying the sources of coevolution.

As for practitioners, we recommend the book Heads Up: How to Anticipate Business Surprises and Seize Opportunities First (McGee 2004). McGee illustrated how to identify and monitor relevant data and information to "predict the present" and thus detect signs of changes early on to seize opportunities. We believe the practices advocated by the author are adequate and relevant in recognizing the driving forces of coevolution.

Our case study explains how in a turbulent high-tech industry, a software company pursued innovation by guiding its offerings to coevolve with new technologies and perceptional/behavioral changes in human actors. Successful innovation involves not only technologies but also human factors. Due to the exploratory nature of this study, our contributions are limited, as stated above. Nonetheless, we hope this study will inspire future research.

7. ACKNOWLEDGEMENT

* The authors gratefully acknowledge the financial support provided by the Ministry of Science and Technology (MOST), Taiwan (Grant No. MOST 106-2410-H-030-070-)

REFERENCE

Backhouse, J. & G. Dhillon. 1995. Managing computer crime: A research outlook. *Computers & Security* 14**,** pp**.** 645–51.

Birkinshaw, J. 2000. *Entrepreneurship in the Global Firm*. London: Sage Publications.

Boulanger, A. 1998. Catapults and grappling hooks: The tools and techniques on information warfare. *IBM Systems Journal* 37, pp. 106–14.

Brennan, L.L. & A.H. Rubenstein. 1995. Applications of groupware in organizational learning. In *Trends in Organizational Behavior,* Vol. 2, ed. C.L. Cooper and D.M Rousseau, Chichester: John Wiley & Sons, pp. 37-49.

Burke, B.E. 2004. Worldwide antivirus 2004-2008 forecast and 2003 vendor shares. In *IDC Market Analysis*, Framingham: IDC.

Burke, B.E., C.J. Kolodgy & Crotty, J. 2007. Worldwide secure content and threat management 2007-2011 forecast and 2006 vendor shares: 1 + 1 = 4. In *IDC Market Analysis*, Framingham: IDC.

Christensen, C.M. 1997. *The Innovator's Dilemma.* Boston: Harvard Business School Press.

Davis, F.D. 1986. *A technology acceptance model for empirically testing new end-user information systems: theory and result*. Boston: Sloan School of Management, MIT.

Dewar, R.D. & J.E. Dutton. 1986. The adoption of radical and incremental innovations: an empirical analysis. *Management Science* 32, pp. 1422–33.

Dijksterhuis, M.S., F.A.J. Van den Bosch & H.W. Volberda. 1999. Where do new organizational forms come from? Management logics as a source of coevolution. *Organization Science* 10, pp. 569–82.

Ettlie, J.E., W.P. Bridges & O'Keefe, R.D. 1984. Organizational strategy and structural differences for radical vs. incremental innovation. *Management Science* 30, pp. 682–95.

Freeman, C. 1982. *The economics of industrial innovation*, 2nd ed. Cambridge: MIT Press.

Hamel, G. 2000. *Leading the Revolution*. Boston: Harvard Business School Press.

Henderson, R. & K. Clark. 1990. Architectural innovation: the reconfiguration of existing product technologies and the failure of established firms. *Administrative Science Quarterly* 35, pp. 9–30.

Hitt, M.A., R.D. Nixon, P.G. Clifford, and K.P. Coyne. 1999. The development and use of strategic resources. In *Dynamic Strategic Resources*, ed. M.A. Hitt, P.G. Clifford, R.D. Nixon, and K.P. Coyne. Chichester: Wiley.

ICSA. 1997. *The Annual Virus Prevalence Surve*y. Mechanicsburg: International Computer Security Association Content Security Labs.

ICSA. 1998. *The Annual Virus Prevalence Survey*. Mechanicsburg: International Computer Security Association Content Security Labs.

ICSA. 2002. *ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001*. Mechanicsburg: International Computer Security Association Content Security Labs.

ICSA. 2005. *ICSA Labs 10th Annual Virus Prevalence Survey*. Mechanicsburg: International Computer Security Association Content Security Labs.

Ireland, R.D. and M.A. Hitt. 1999. Achieving and maintaining strategic competitiveness in the 21st century: the role of strategic leadership. *Academy of Management Executive* 13, pp. 43–57.

Lewin, H. W. and H.W. Volberda. 1999. Prolegomena on coevolution: A framework for research on strategy and new organizational forms. *Organization Science* 10, pp. 519–34.

Lyons, D. 1998. The decline and fall of Lotus. *Forbes* 162, pp. 106–107.

MacKenzie, D. and J. Wajcman. 1985. *The Social Shaping of Technology: How the Refrigerator Got its Hum.* Milton Keynes: Open University Press.

Mark, G. 1993. Guarding all servers. *Network World* 10: 59–61.

McGee, K.G. 2004. *Heads Up: How to Anticipate Business Surprises and Seize Opportunities First.* Boston: Harvard Business School Press.

Moschovitis, C. J. P., H. Poole, T. Schuyler, and T.M. Senft. 1999. *History of the Internet: A Chronology, 1843 to the Present.* Santa Barbara: ABC-Clio Inc.

Podolny, J.M. and T.E. Stuart, T.E. 1995. A role-based ecology of technological change. *American Journal of Sociology* 100, pp. 224–60.

Richardson, R. 2003. *2003 CSI/FBI Computer Crime and Security Survey*. Available at http://www.gocsi.com.

Rogers, E. M. 1995. *Diffusion of Innovations*, 4th ed. New York: Free Press.

Schumpeter, J. A. 1934. *The Theory of Economic Development.* Cambridge: Harvard University Press.

Strauss A. & J. Corbin. 1990. *Basics of Qualitative Research.* Newbury Park: Sage.

Sundbo, J. 1998. *The Theory of Innovation.* Cheltenham: Edward Elgar Publishing.

Sundbo, J. 2001. *The Strategic Management of Innovation.* Cheltenham: Edward Elgar Publishing.

Tushman, M. & C. O'Reilly III. 1997. *Winning Through Innovation: A Practical Guide to Leading Organisational Change and Renewal.* Boston: Harvard Business School Press.

Tushman, M.L. & P. Anderson. 1986. Technological discontinuities and organizational environments. *Administrative Science Quarterly* 31, pp. 439–650.

Utterback, J. & W. Abernathy. 1975. A dynamic model of process and product innovation. *Omega* 13, pp. 639–656.

Vance, M. 1996. Firewalls to offer viral protection. *Datamation* 42, pp.11–12.
Venkatesh, V. and F.D. Davis. 2000. A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science* 46, pp.186–204.

Van Maanen, J. 1979. Reclaiming qualitative methods for organizational research: a preface. *Administrative Science Quarterly* 2, pp. 520–527.

Williams, R. & D. Edge. 1999. The social shaping of technology. *Research Policy* 25, pp. 865–899.

Yin, R. 1983. *Case Study Research: Design and Method.* Newbury Park: Sage.