International Journal of Business and Management; Vol. 8, No. 12; 2013
ISSN 1833-3850 E-ISSN 1833-8119
Published by Canadian Center of Science and Education

Using System Dynamics to Investigate the Effect of the Information Medium Contact Policy on the Information Security Management

Pei-Chen Sung[1] & Chien-Yuan Su[1]

[1] Department of Information Management, National Chung Cheng University, Chia-yi, Taiwan, R. O. C.

Correspondence: Pei-Chen Sung, Department of Information Management, National Chung Cheng University, No. 168, Sec. 1, University Rd., Min-Hsiung Township, Chia-yi County 62102, Taiwan, R. O. C. Tel: 886-5-272-0411. E-mail: pcsung@mis.ccu.edu.tw

Received: April 1, 2013 Accepted: April 24, 2013 Online Published: May 24, 2013

doi:10.5539/ijbm.v8n12p83 URL: http://dx.doi.org/10.5539/ijbm.v8n12p83

Abstract

Computer viruses remain the information security threat for business and result a devastating effect on business continuity and profitability. In order to deploy antivirus countermeasures, it is necessary to understand and explore the computer virus propagation. This research explored further the users who contact with media and discuss information security controls, including management and technical. First, we propose the computer viruses propagation model and analysis from system viewpoint. Second, we explore and evaluate the effectiveness of preventive countermeasures. Finally, we suggest several considerations for manager to practice. The simulation results show that users contact with media for network had a significant effect on infection rate and policy enforcement has powerful influence than firewall on restrain infection rate. Based on these results, we suggest: (1) information security management policy development takes precedence over the physical security; (2) it is very important to identify all assets, define the classification of assets, and identify security roles and responsibilities of employees; (3) it is necessary to audit regularly the configurations and the parameters of security techniques; (4) the operating system and the application software on hosts and servers should be updated and patched regularly; (5) the removable storage and removable/mobile access media should be restricted.

Keywords: information security management, ISO/IEC 27001, system dynamics, computer virus propagation, antivirus countermeasures

1. Introduction

Today, more and more enterprises depend heavily on information and information technology to create a lot of innovative services. In most cases, information has become the vital ‘asset’ called ‘information asset’ or ‘intellectual asset’ for enterprises. However, information is continuously being threatened to be lost, stolen, accessed (physically or otherwise), blocked, misused or destroyed by people, computer viruses, malwares, natural disasters (e.g. earth quake), man-made disasters (e.g. 911 attacks), etc. It is particularly important to protect these assets to ensure their confidentiality, integrity and availability. Obviously, managing security of information is as important as managing the core business.

According to the Computer Security Institute (CSI) of Computer Crime and Security Survey from 1999 to 2010, virus attacks have topped the list of attack types (Computer Security Institute [CSI], 2010). The annual information security reports from the CSI also show that viruses caused the biggest financial loss among all computer security incidents in industry (CSI, 2003-2006). This result of report is shown that attacks of the computer virus are incessant and incremental. This reason of the phenomenon may be the computer viruses awareness and prevention is deficient in users. Therefore, understanding and exploring the computer virus propagation is necessary either individuals or organizations especially in the information security policies construction and development.

Information security management (ISM) research is a relatively new issue. Most research adopts case study or survey research. Case studies can provide in-depth data on an object of study and spark ideas for further research, but we can’t assume it will apply to all others with the same condition. Survey research used questionnaires or interviews to efficiently collect data from many people. These surveys have been mostly using quantitative and primarily statistical methods. Previous research indicated that the slight response rate which uncovered that the main reasons that the related information security is regarded as confidentiality and the policy of information secrecy is implemented extensively in enterprise. These above-mentioned actualities, the sufficient quantity of received survey is more arduous, hence, the amount of received survey in information security research generally are slighter than other research issues (Albrechtsen & Hovden, 2009; Department of Trade & Industry, 2004; Kotulic & Clark, 2004; Vance, Siponen, & Pahnila, 2012). On the other hand, the majority of studies on computer virus propagation published in the IS security literature a technical perspective and lack of management perspectives. In addition, user behaviors must be taken into account because "people" are always the key factor for the success of information security management in companies and organizations regardless of its size, location, culture or type of business (Eminağaoğlu, Uçar, & Eren, 2009). Based on limitations of the research methods and tools in information security research, we attempt to adopt other research method to surmount these obstacles.

In this paper, we present a virus propagation model based on SEIR (Susceptible-Exposed-Infectious-Recovered) epidemic model and develop with the use of system dynamics methodological approach to investigate the effect of users contact with media on computer virus propagation. System dynamics methodological approach shows how structure, policies, decisions and time delays within systems are interrelated and influence growth and stability (Lee & Tunzelmann, 2005). It is considered that the system function is determined by its structure, and the system behavior pattern depends on the dynamic structure and the internal feedback mechanisms of the system. The first step of implement ISM is establishing complete information security policy. ISO/IEC 27001 provides the form of guidance and recommendations for information security management, and indicates the importance of users contact with media in against computer viruses. However, most studies have focused on deployment and access control in facilities. We should notice that communication media, electronic storage and transmission of information are increase in the growth rate. Computer viruses can spread through network and media. A study by the present researcher proposed a computer virus propagation model and also discovered there was a significant effect for contacting with media in infection rate (Sung, Ku & Su, 2013). It is therefore the intent of the present study to explore the impact extent of users contact with media on computer virus propagation, and propose considerations. Our model will be generalized to represent the behavior of general computer viruses, and incorporated into user behaviors and technical security solutions to study virus propagation from a managerial perspective.

2. Literature Review

2.1 System Dynamics

System dynamics (SD) was developed in 1950 by Jay W. Forrester of Massachusetts Institute of Technology (MIT) which is the study of behavior of complex systems over time developed to model complex continuous systems for improving management policies and organizational structures (Forrester 1961, 1968). SD is an approach that able to deal with non-line problems, information feedbacks, time delays and complex systems, and its methodology put emphasis on conceptualization, formulation and simulation (Richardson, 1996). SD simulation is performed to learn about the dynamics of the system behavior that may impact the planning solution by using closed-loop feedback and to design policies to improve system performance.

SD methodology is included two stages. In the first stage, the qualitative system model is developed in the form of a causal loop diagram which captures the major feedback mechanisms. Causal loop diagrams play two important roles in SD. First, during model development, they serve as preliminary sketches of causal hypotheses and secondly, they can simplify the representation of a model (Georgiadis, Vlachos, & Iakovou, 2005). In the second stage, the qualitative model is transformed into a stock and flow diagram and is calibrated for quantitative analysis using simulation techniques (Wolstenholme & Coyle, 1983; Wolstenholme, 1994). The structure of a system flow diagram contains stock and flow variables, also known as the stock flow diagram. Stock variables are the accumulations (i.e. inventories), while flow variables represent the flows in the system (i.e. order rate). SD modeling effort can improve understanding of the relationships between feedback structures and dynamic behaviors of a system so that policies for improving problematic behavior may be developed (Richardson & Pugh, 1981). Nowadays, SD models use graphical simulation programs to represent relationships between components of a system using stocks and flows, and support the analysis and study of these systems. Therefore, SD models allow managers to test alternative assumptions, decisions and policies (Suryani, Chou, Hartono, & Chen, 2010).

In the past decades, SD has been widely utilized to study dynamic behavior of various social systems and has been applied to policy analysis and design both in the public and private sectors (Casey & Töyly, 2012). Information security management is complexity because that involves three types of security controls: technical, policy and human controls (Botha & Gaadingwe, 2006; Dhillon & Moores, 2001; Sveen, Torres, & Sarriegi, 2009). The spread of computer viruses is a nonlinear dynamic system, similar to the spread of epidemics in human populations (Kephart & White, 1993; Pastor-Satorras & Vespignani, 2001). It is regarded as a complex system. Consequently, SD is suitable for applied in information security management and computer virus propagation.

2.2 Computer Viruses Prevention in ISO-27001 Standard

ISO/IEC 27001 is described as a suitable model for ISM and an appropriate vehicle for addressing ISM issues in organizations (Dhillon & Moores, 2001). It consists of the 11 control sections and 133 security controls for practitioners to use. However, there is no specific chapter for defense against computer viruses implementations in ISO/IEC 27001. In several chapters, the related security controls have been proposed in the security management view which is in the "Protection against malicious and mobile code", "Technical vulnerability management", and "Reporting information security events and weaknesses". These security controls are listed in Table 1.

Table 1. The controls in ISO/IEC 27001 about computer virus prevention

Security Control	Description
Controls against Malicious Code (10.4.1)	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented
Control of technical vulnerabilities (12.6.1)	Timely information about technical vulnerabilities of information systems being use should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk
Reporting information security events (13.1.1)	Information security events should be reported through appropriate management channels as quickly as possible

2.2.1 Controls against Malicious Code

In chapter 10.4 of "Protection against malicious and mobile code", the subsection 10.4.1, "Controls against malicious code" shows if software and information processing systems are vulnerable, malicious code would be introduced. Manager should establish a policy to protect the dangers of malicious code. For example, use detection software, update anti-virus software and change management controls.

2.2.2 Control of Technical Vulnerabilities

In Chapter 12.6.1 of ISO 27001, is for the technical vulnerability management. This control shows that a correct and complete inventory of assets is necessity for technical vulnerability management. Software vendors and employees within the organization responsible for the software have responsibility for supporting technical vulnerability management.

2.2.3 Reporting Information Security Events

In Chapter 13.1.1 of ISO 27001, is for the information security incident management that highlights the need for a formal information security event reporting procedure should be established. All employees, contractors and third party should be required to report any information security events as quickly as possible.

3. Modeling

In this research, we use SD methodology to develop the computer virus propagation model. First, we construct and analyze the causal loop diagram to describe the general computer virus propagation. Then, build up the stock and flow diagram for simulation, results, and recommendations. These stages are explored in detail below.

3.1 Causal Loop Diagram

A causal loop diagram is constructed to represent the relationships between these variables of the computer virus propagation. Figure 1 shows the causal loop diagram of computer virus infection flow. The structure can be described by 1 positive loop (R) and 1 negative loop (B).

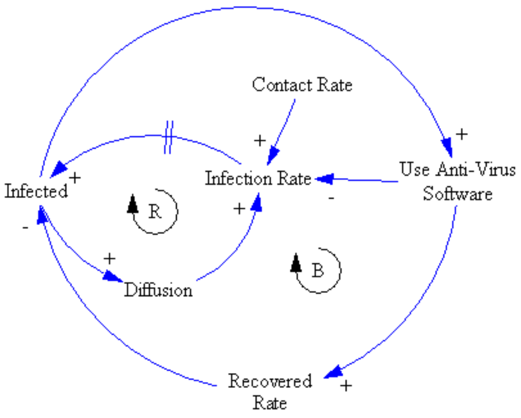


Figure 1. Causal loop diagram of computer virus propagation

In general the major reason of user’s devices infected is clicked malicious link. Each device is connected to the network could be mutually infected. Computer viruses can spread through channels, such as USB devices, e-mail, instant messengers (IM), Peer-to-Peer (P2P) file sharing, and online social network services (SNS). Computer system may be infected by clicking incidentally or wrongly an attachment of malicious executable file or malicious URL. The Contact Rate indicated the frequency of devices contacted network (e.g. Internet and Intranet) and external media (e.g. USB devices and other disks). In general users easy to be attracted by the interesting link and trust the messages that send by their friends. Due to linking and messages may be forged and included malicious code, such as ActiveX. Once users click on, the devices will be infected. Unfortunately, when user discovers that his device has been infected, the virus would have spread out. Because of computer viruses will hide themselves in device for some time preceding attack; user can’t immediately detect (R).

On the other hand, in order to recover infected computers, anti-virus software adoption is regarded as one of the most effective approaches (Forrest, Hofmayer, & Somayaji, 1997). Anti-virus software adopted can reduce the probability of infection and infection rate. If user finds his device was infected, he will use anti-virus software to remove the viruses (B). The summary of the feedback loops of computer virus propagation is presented in Table 2.

Table 2. Summary of the feedback loops of computer virus propagation

Code	Loop Content	Loop Effect
R	Infected—Diffusion—Infection Rate—Infected	Computer viruses diffusion
B	Infected—Use Anti-Virus Software—Recovered Rate—Infected	Use anti-virus tools to remove computer viruses

Note: R represents reinforcing; B represents balancing.

3.2 Causal Loop Diagram Analysis

According to Figure 1, we find that reducing the probability of infection is control over contact rate. Users adopt anti-virus software to reduce the probability of infection; however, the source of problems is contact rate. Malicious and mobile code can spread through many channels on Internet (e.g. e-mail, IM, and Online Social Networking) and are clicked or attached incidentally to infect most of IT devices in the network. Through sending or sharing files on these channels, malicious codes (or URL) can invade devices to spread computer viruses. The system may be infected by clicking incidentally or wrongly. Therefore, the frequency of user contact network and external media is crucial to determine whether user’s devices infected.

There has been a rapidly growing interest in the use of epidemiological models for understanding of computer viruses spreading since the pioneering work by Murray (1988). Following this idea, many epidemic models of computer viruses have been proposed. Some defects of previous epidemic models of computer viruses were reported recently:

1) An infected computer which is in latency can infect other computers through files downloading or files copying. Unfortunately, previous computer virus models failed to consider this passive infectivity (Yang, Yang, Zhu, & Wen, 2013);

2) Previous works on malware modeling assume that the infection rate is a constant (Fen, Liao, Han, & Li, 2013) and random. Not only constant infection rate, but random infection rate, however, there are unsuitable for virus propagation in computer networks (Yuan, Wu, & Chen, 2009);

3) Removable storage devices provide a way other than the Internet for the spread of viruses. However, nearly all previous models of computer virus propagation ignore the effect of removable devices on the spread of viruses (Yang & Yang, 2012);

On the other hand, it is inevitable that mention of antivirus countermeasures in discussing computer viruses threats. According to 2010/2011 CSI Computer Crime and Security Survey (CSI, 2010), in the use of security technology, anti-virus software had the highest utilization rate of 97.0%, followed by the application of firewall (94.9%). Therefore, combination of computer virus propagation models and antivirus countermeasures is necessary.

Recently, some researchers proposed new models to overcome above defects (Table 3). However, none of these models has considered the viewpoint of ISM policies. This paper aims to understand the effect for contacting with media in infection rate. The latent period, dynamic infection rate, antivirus countermeasures, ISM policies enforcement are considered in our model.

Table 3. Summary of Epidemic model in preceding information security researchers

Authors (Year)	Epidemic model	Focus factors
Yuan, Chen, Wu & Xiong (2009)	SEIR	Latent period, Antivirus countermeasures
Han & Tan (2010)	SIRS	latent and temporal immune periods
Song, Jin, Sun, Zhang & Han (2011)	SIR	Removable devices
Mishra & Pandey (2012)	SSIP	Anti-virus software
Fen, Liao, Han & Li (2013)	SIRS	Infection rate

On the basis of above analysis, we focus on the contact rate that users contact with network and external media respectively. Further, we consider that the effectiveness of the firewall, and the duration of the users contact the network and external media.

3.3 Stock and Flow Diagram

In SD methodology, the causal loop diagram and the stock and flow diagram are main tools. The causal loop diagram is represented the structure of a system and major feedback mechanisms, the diagram in this paper is illustrated in Figure 1 in above section. The stock and flow diagram is the mathematical model that can be representing equations to exhibit the dynamic behavior between the factors of the objective system. Murray (1988) considered that the behavior of a virus program is analogous epidemic and suggested that understanding behavior of computer viruses through the epidemic model is more feasible and useful. In this paper, the SEIR (Susceptible-Exposed-Infective-Recovered) model (Anderson & May, 1992) was adopted because it contents exposed state (E) and takes the latent period into consideration. In this section, we will interpret explicitly the development of stock and flow diagram and the procedure of analysis in this research. The notation list is given in Table 4.

Table 4. Notation list

Variable	Initial Value	Definition
FINAL TIME	144	Final time of the simulation (Unit: hour)
INITIAL TIME	0	Begin time of the simulation (Unit: hour)
Susceptible (*S*)	999 (S_0)	The number of susceptible devices (Unit: device) Initial Value = Total Device - Initial Exposed - Initial Exposed
Exposed (*E*)	1 (E_0)	The number of infected asymptomatic devices (Unit: device)
Infectious (*I*)	0 (I_0)	The number of infective devices with onset of symptoms not quarantined (Unit: device)
Recovered (*R*)	0 (R_0)	The number of devices that will not be infected again. This class including immunity and recovery (Unit: device)
Total Device (*N*)	1000	The sum of amount of susceptible devices, exposed devices, infectious devices and recovered devices. (Unit: device) N = S + E + I + R
Infection Rate (*IR*)		The transformation rate of susceptible individuals to exposed individuals (Unit: device/hour)
Exposed to Infected Rate (*EIR*)		The transformation rate of exposed individuals to infectious individuals (Unit: device/hour)
Exposed to Recovered Rate (*ERR*)		The transformation rate of exposed individuals to recovered individuals (Unit: device/hour)
Contact Rate for Network	4	The duration of devices contacted network (including Internet, Intranet, etc.) (Unit: hour)
Contact Rate for External Media	1	The duration of devices contacted external media (ie. USB devices and other disks) (Unit: hour)
Probability of Contact Network with Malicious	0.4	The probability of user clicks incidentally or wrongly an attachment of malicious executable file or malicious URL
Probability of Contact External Media with Malicious	0.6	The probability of user contact external media including malicious files or programs
Firewall	0	The effectiveness of Firewall that user deploys to fight with computer viruses
Policy Enforcement	0	The implementation of the contact policy in the information security
start	1	Beginning time of contact network
start1	3	Beginning time of contact external media
repeattime	5	Time interval of contact network
repeattime1	4	Time interval of contact external media
e	0.5	The probability of a susceptible device gets infected when connected to exposed device
Infectivity	0.7	The probability of a susceptible device gets infected when connected to an infectious device
Average Durations of Latency Periods	12	The period between infection and the first obvious damage to the host system (Unit: hour)
Probability of Use AntiVirus Software	0.5	The ratio of users actively use antivirus software

The stock and flow diagram is constructed by stock variables, flow variables, auxiliary variables and constants variables. A stock variable (symbolized by rectangle) represents a point where content can accumulate and deplete. A flow variable (symbolized by valve) is a rate of change in a stock variable and it represents an activity, which fill in or drain the stock variable. Some examples of such activities are infects in a population or recovers from a population, improvement of capability. An auxiliary/constant variable can store an equation or a constant. Finally, the connectors, represented by simple arrows, are the information links representing the cause and effects within the model structure, while the double line arrows represent physical flows. Double lines across the arrows indicate delayed information.

The computer virus propagation model, namely stock and flow diagram, is developed by Vensim PLE in this research and illustrated in Figure 2. In this research, susceptible, exposed, infectious and recovered are principal stock variables; infection rate, exposed to infected rate, exposed to recovered rate and recovery rate are flow variables. Total device, contact rate for network, probability of contact network with malicious, infectivity and average durations of latency periods, etc., are auxiliary/constant variables. Contact rate for network link infection rate by simple arrow because the relation of these two variables is the cause and effect. Susceptible devices flow to exposed devices represents physical flows and they link by the double line arrows. Following the classic assumption, the population of the recovered class implies permanent immunity that is there is no return of the removed individuals into the susceptible class. The following equations are introduced to facilitate the model description.

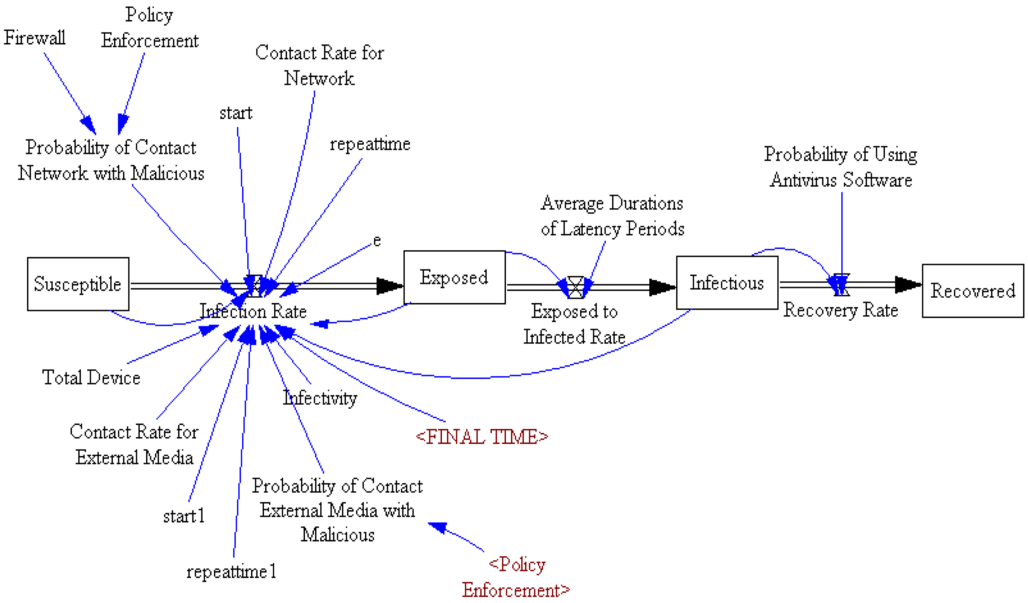


Figure 2. Stock and flow diagram for computer virus propagation

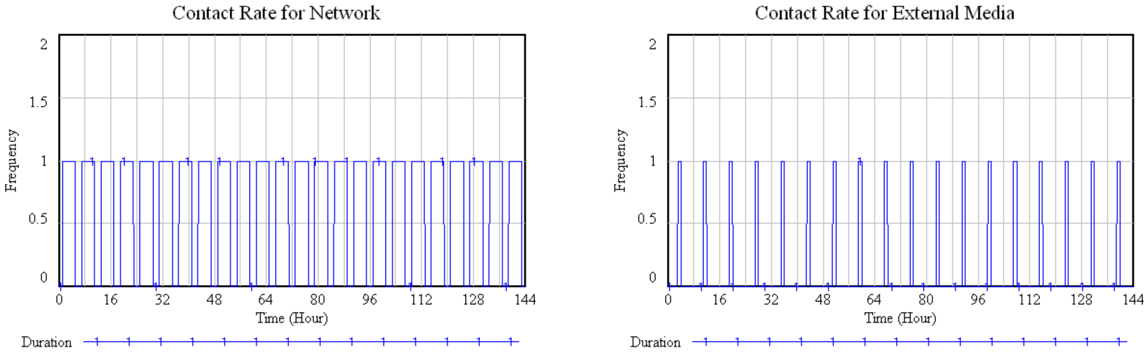
In order to fight with computer viruses, users deploy antivirus countermeasures, such as firewall, to fight with computer viruses. Information security policy specifies how the rules are to be followed. These measures help to mitigate computer viruses threats consequently. We assume the initial value of probability of contact network with malicious and probability of contact external media with malicious are 0.4 and 0.6 respectively. Therefore, the equations are:

Probability of Contact Network with Malicious = IF THEN ELSE(Firewall=0: AND: Policy Enforcement=0, 0.4, 1-MAX(Firewall, Policy Enforcement)) (1)

*Probability of Contact External Media with Malicious = IF THEN ELSE(Policy Enforcement = 0, 0.6, 0.6*Policy Enforcement)* (2)

Computer system may be infected by clicking incidentally or wrongly an attachment of malicious executable file or malicious URL. The computer virus in latency period and the devices have been infected may infect other devices. We make the simplifying assumption that users contact the network and external media is a routine work. The frequencies are shown as Figure 3. Therefore, the equation of infection rate is:

Infection Rate = IF THEN ELSE(Probability of Contact Network with Malicious=0, Susceptible((Exposed*e+Infectious*Infectivity)/Total Device)+PULSE TRAIN(start1, Contact Rate for External Media, repeattime1, FINAL TIME)*Probability of Contact External Media with Malicious, Susceptible*((Exposed*e+Infectious*Infectivity)/Total Device)*PULSE TRAIN(start, Contact Rate for Network, repeattime, FINAL TIME)*Probability of Contact Network with Malicious+PULSE TRAIN(start1, Contact Rate for External Media, repeattime1, FINAL TIME)*Probability of Contact External Media with Malicious)* (3)



(a) (b)

Figure 3. The frequency and duration of devices contacted (a) network and (b) external media

After durations of latency periods, exposed devices will become infectious devices. The capacity of antivirus company can reduce average durations of infectivity periods, but it can not affect the latency period of the computer virus. Hence average duration of latency periods is not influenced by any variables. Therefore, the equation of Exposed to Infected Rate is:

Exposed to Infected Rate = Exposed / Average Durations of Latency Periods (4)

This paper assumes that anti-virus software including the newest virus signatures and could be effective against attack by computer viruses. If user finds his device was become infective, he/she will use antivirus software to remove computer virus. The equation of Recovery Rate is defined as:

*Recovery Rate=Infectious*Probability of Using Antivirus Software* (5)

According above definitions, the equations of the stock variables, susceptible, exposed, infectious and recovered respectively are:

$$Susceptibl\ e(t) = \int_0^t [-\ IR(s)]ds + S_0 \tag{6}$$

$$Exposed\ (t) = \int_0^t [IR(s) - EIR(s)]ds + E_0 \tag{7}$$

$$Infectious\ (t) = \int_0^t [EIR(s) - RR(s)]ds + I_0 \tag{8}$$

$$\mathrm{Re\ cov}\ ered\ (t) = \int_0^t [RR(s)]ds + R_0 \tag{9}$$

4. Results and Discussion

4.1 Model Validation

Model validation focuses on justifying the reliability of the model and providing confidence for model application. The validation of a SD model usually involves: (1) structural validity, and (2) behavior validity. Structural validity includes comparative evaluation of each model equation against its counterpart in the real system or in the relevant literature (Vlachos, Georgiadis, & Iakovou, 2007). Model behavior validity refers to how well the model-generated behavior reproduces or mimics the observed behavior of the real system (Khan, Yufeng, & Ahmad, 2009; Sterman, 2000).

4.1.1 Structural Validity

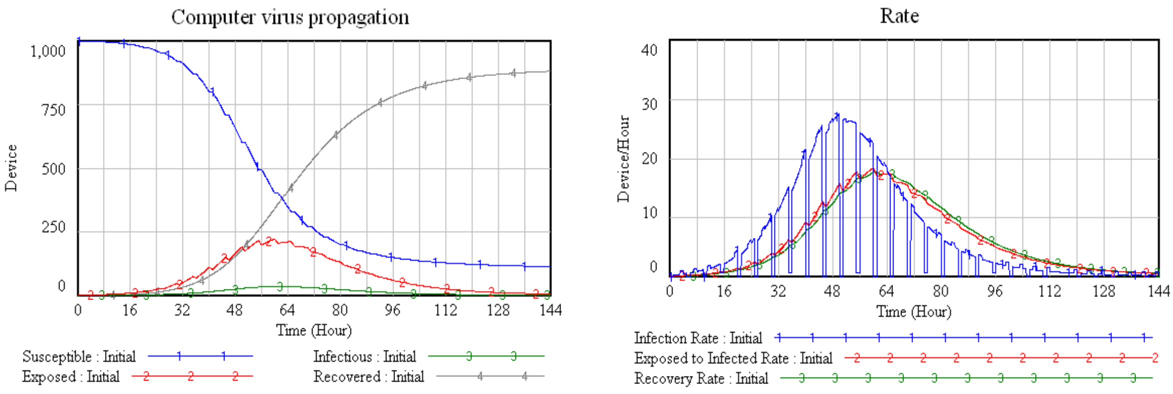
The SEIR model has used for modeling the spread of computer virus, though its mathematical complexity and has not been widely used. For example, based on SEIR model, Yuan and Chen (2008) and Yuan et al. (2009) proposed E-SEIR model to gain insights of virus propagation in networks with Point-to-Group information sharing patterns; Mishra and Pandey (2011) presented SEIRS model for the transmission of worms in computer network through vertical transmission. Furthermore, the mathematical relationships for our model were based on epidemiology-based models. Hence the structural validity of our research model is supported by literature and satisfied the requirements of the SD.

4.1.2 Behavior Validity

Behavior validity determines how consistently model outputs match real world behavior (Barlas, 1996). The usefulness of validity is running the simulation with the actual, historical data. Unfortunately, due to the non-existence data, we compare the behavior of our model with the behavior of other research model. The result of this research model behavior that is shown as Figure 4(a) is similar to previously research (Yuan & Chen, 2008; Yuan et al. 2009). Therefore, we conclude that the simulation model of this research is high behavior validity.

4.2 Initial Results

These assumptions of this research are: (1) users adopt antivirus software with the latest virus signatures and could be effective against attack by computer viruses; (2) there are no vulnerabilities in operation system because user has already patched. The results of initial are shown as Figure 4. The propagation trend of SEIR model is shown in Figure 4(a) and the dynamic of rates are shown in Figure 4(b). Users do not contact network and external media continuously; hence computer virus propagates at a slower speed and infection rate is oscillation. Because probability of use antivirus software is 0.5, the number of recovered class, R, is much smaller than total devices. The number of infectious class is not apparent because the exposed devices transform to infectious devices after latent period.

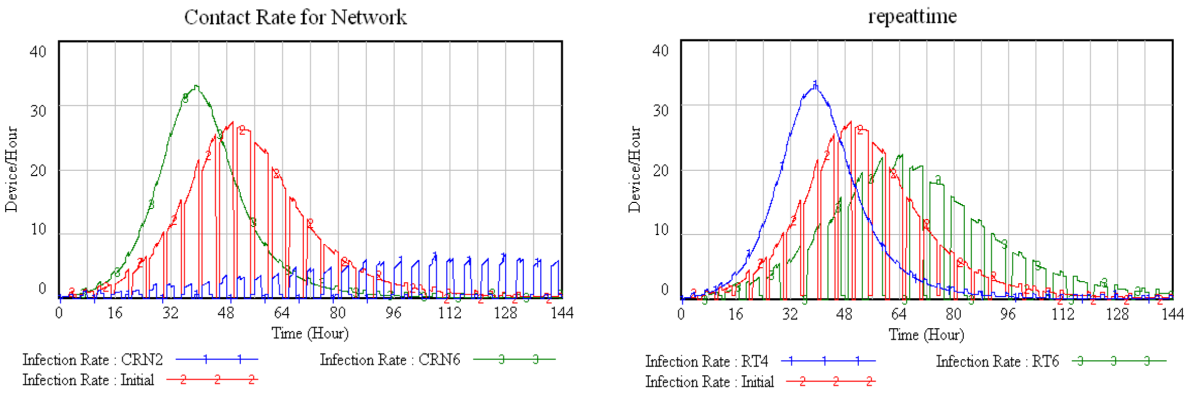


(a) (b)

Figure 4. Initial simulation results

4.3 The Effects of Contact Rate for Network and External Media

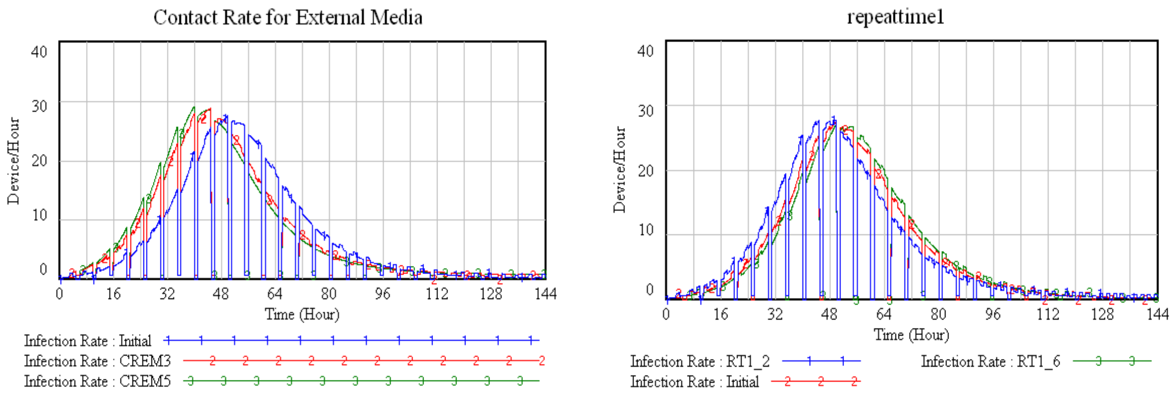
In this section, the effects of contact rate on computer virus propagate are explored in Figure 5 and Figure 6. We assume probability of contact network with malicious is 0.4. In Figure 5(a), plotted trends 1, 2, and 3 show the changes in the infection rate based on contact rate for network values of 2 (CRN2), 4 (Initial) and 6 (CRN6) respectively. Obviously, the longer the duration of devices contacted network, the more significant that devices would be infected. In Figure 5(b), plotted trends 1, 2, and 3 show the changes in the infection rate based on repeattime values of 4 (RT4), 5 (Initial) and 6 (RT6) respectively. The more frequency contact network, the more significant that devices would be infected.



(a) (b)

Figure 5. The effects of (a) contact rate for network and (b) repeattime

The impact of contact rate for external media on computer virus propagation is shown in Figure 6. In our initial scenario, probability of contact external media with malicious is 0.6. In Figure 6(a), plotted trends 1, 2, and 3 show the changes in the infection rate based on contact rate for external media values of 1 (Initial), 3 (CREM3) and 5 (CREM5) respectively. In Figure 6(b), plotted trends 1, 2, and 3 show the changes in the infection rate based on repeattime1 values of 2 (RT1_2), 4 (Initial) and 6 (RT1_6) respectively. Users contact with external media will affect the infection rate but this effect is not significant.



(a) (b)

Figure 6. The effects of (a) contact rate for external media and (b) repeattime1

The simulation results indicate that contact for network affects the infection rate is more significant than contact for external media. Web-based systems are increasingly adopted in organizations. If networks were open, then anyone can easily access and their devices would be infected. Therefore, managers must institute the network utilization policy for all employees. For example, define a standard in accordance with employees's power or working scope. We can improve the organizational security by define and establish roles and responsibilities of staffs, enhance the awareness and training, strengthen the physical access and control, etc. The following protection mechanisms must be considered and employed:

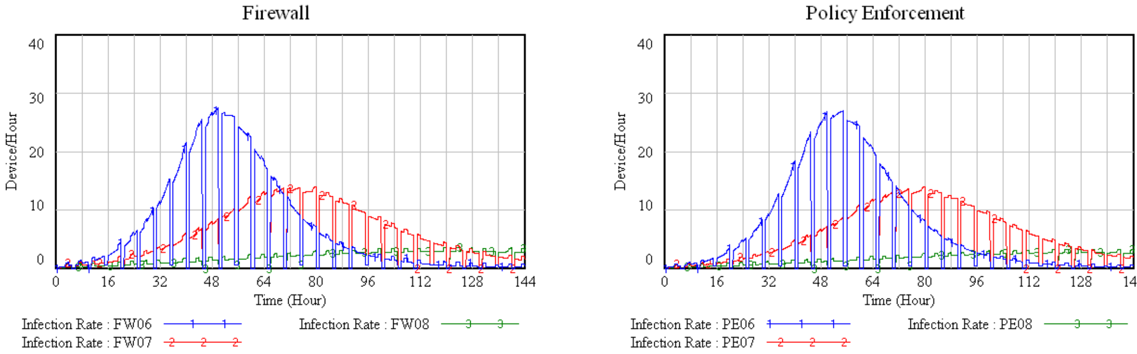
- To ensure the assets receive an appropriate level of protection, manager should identify all assets and define the classification of assets;
- The authentication schemes are not only performed as the outsiders or the new-comers request these internal services, but also as the insiders request these services on the external servers;
- The removable storage and removable/mobile access media should be restricted. If there are requisite, they should be restrained by classified persons;

- Employing techniques such as anti-virus system, content filter and malicious code detection mechanism, to ensure the information security in the data transmission between or in networks.

4.4 The Effects of Firewall and Policy Enforcement

More and more people access information over Internet and mobile networks, and many messages are sent through e-mail or social network. As websites are vulnerabilities and existing malicious URL, computer system may be infected by clicking incidentally. We consider the probability of contact network/external media with malicious that indicated people adopt technical security solutions such as firewalls to solve information security problems and implement information security policy. Firewall are implemented more efficiently, the value of probability of contact with malicious is lower. Policy enforcement would mitigate the risk of computer viruses threats. First, we consider influences of firewall on the dynamics of infection rate. The simulation results are shown in Figure 7(a). The plotted trends 1, 2, and 3 show the changes in the infection rate based on the effectiveness of firewall values of 0.6 (FW06), 0.7 (FW07) and 0.8 (FW08) respectively. Second, we consider influences of policy enforcement on the dynamics of infection rate. The simulation results are shown in Figure 7(b). In Figure 7(b), plotted trends 1, 2, and 3 show the changes in the infection rate based on the level of compliance with the policy values of 0.6 (PE06), 0.7 (PE07) and 0.8 (PE08) respectively. Compared with the optimization of Figure 7(a) and 7(b), the trends of infection rate is shown in Figure 8. The result show that policy enforcement has powerful influence than firewall on restrain infection rate.

This result has highlighted the importance of ISM and revealed an important challenge for ISM. It is difficult to implement security controls when people do not have enough orientation or education about IT security practices. In addition, it is difficult to decide how security controls could be integrated in the existing infrastructure, especially the organization has many interconnected systems, such as servers, networks and databases. The complexity of networks and systems is also a challenge when implementing security controls in organizations. Although various network security techniques such as firewalls and intrusion detection systems have been developed for detection and prevention of attacks, there are few people to maintain and audit the security rules.



(a) (b)

Figure 7. The influences of (a) firewall and (b) policy enforcement on the dynamics of infection rate

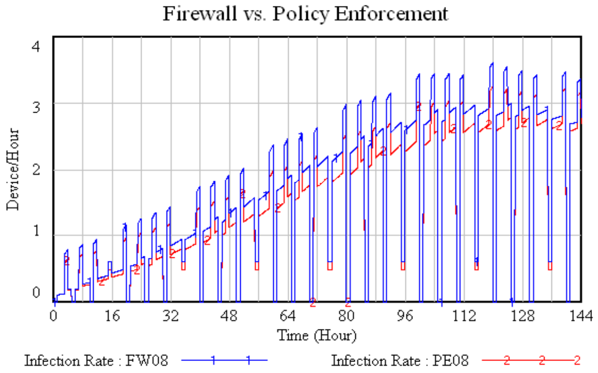


Figure 8. The influences of infection rate (FW08: Firewall = 0.8; PE: Policy Enforcement = 0.8)

According to above discussions, for detection and prevention of computer viruses attacks, we suggest the following considerations:

- Establish security culture and enhance education and training of information security;
- According to the policies of organizations, establishing the firewalls or security gateways avoids illegal access;
- The configurations and the parameters of firewalls should be audited regularly;
- The operating system and the application software on hosts and servers should be updated and patched regularly.

5. Conclusions

In this paper, we develop a SEIR model using SD method for computer viruses propagation analysis by taking into account the effect of antivirus countermeasures and focus on the contact rate that users contact with network and external media respectively from the viewpoint of information security management policies. We assume that users adopt antivirus software with the latest virus signatures and there are no vulnerabilities in operation system. By contrast, our main contributions include the following: (1) we combine the viewpoint of ISM with computer virus propagation model to overcome the lack of managerial insights in previous research; (2) we consider the influence of antivirus countermeasures on computer virus propagation in different stage. Anti-virus software and firewall are the top list people have deployed to fight with computer viruses in the state transition path from S to E and I to R. The results show that: (1) contact for network affects the infection rate is more significant than contact for external media; (2) policy enforcement has powerful influence than firewall on restrain infection rate. The results have highlighted the importance of information security management for organizations. Information security includes both technological and human issues. Security techniques are not sufficient in mitigating computer viruses threats without management policies. Though the security techniques would be developed rapidly and have effects remarkably, management and audit policies should be enforced and continually monitoring, maintaining and improving.

Based on limitations of the research methods and tools in information security research, we adopt SD method to surmount these obstacles, and provide a new path in the research of information security management. The findings of this study include managerial implications. Protecting information often requires the application of some technology, but it always requires use of people and processes (Broderick, 2006). We should not overlook the fact that the electronic applications in businesses and sharing of information on network systems have increased. Therefore, a set of ISM policy must be established, including security requirements, asset management, roles and responsibilities, security awareness training and policy education, and compliance, etc, and should be stressed in operating activites. After implementing security techniques, configurations and the parameters of facilities should audit regularly in accordance with policy. Much remains to be done, then, but we anticipate that the study will generate important findings in the fields of information security management.

References

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476-490. http://dx.doi.org/10.1016/j.cose.2009.01.003

Anderson, R. M., & May, R. M. (1992). *Infectious diseases of humans: Dynamics and Control*. USA: Oxford University Press.

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. *System Dynamics Review, 12*(3), 183-210. http://dx.doi.org/10.1002/(SICI)1099-1727(199623)12:3<183::AID-SDR103>3.3.CO;2-W

Botha, R., & Gaadingwe, T. (2006). Reflecting on 20 SEC conferences. *Computers & Security, 25*(4), 247-256. http://dx.doi.org/10.1016/j.cose.2006.04.002

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report, 11*(1), 26-31. http://dx.doi.org/10.1016/j.istr.2005.12.001

Casey, T. R., & Töyli, J. (2012). Mobile voice diffusion and service competition: A system dynamic analysis of regulatory policy. *Telecommunications Policy, 36*(3), 162-174. http://dx.doi.org/10.1016/j.telpol.2011.07.002

Computer Security Institute. (2003). *CSI Computer Crime & Security Survey.* Retrieved from http://www.yle.fi/mot/kj040524/fbiraportti.pdf

Computer Security Institute. (2004). *CSI Computer Crime & Security Survey.* Retrieved from http://gocsi.com/sites/default/files/uploads/FBI2004.pdf

Computer Security Institute. (2005). *CSI Computer Crime & Security Survey.* Retrieved from http://gocsi.com/sites/default/files/uploads/FBI2005.pdf

Computer Security Institute. (2006). *CSI Computer Crime & Security Survey.* Retrieved from http://gocsi.com/sites/default/files/uploads/FBI2006.pdf

Computer Security Institute. (2010). *CSI Computer Crime & Security Survey.* Retrieved from https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

Department of Trade & Industry (DTI). (2004). *Information security breaches survey.* Retrieved from http://www.galenaitgroup.com/members/downloads/DTi%20Information%20Security%20Survey%202004.pdf

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security, 20*(8), 715-723. http://dx.doi.org/10.1016/S0167-4048(01)00813-6

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report, 14*(4), 223-229. http://dx.doi.org/10.1016/j.istr.2010.05.002

Feng, L., Liao, X., Han, Q., & Li, H. (2013). Dynamical analysis and control strategies on malware propagation model. *Applied Mathematical Modelling,* In Press. http://dx.doi.org/10.1016/j.apm.2013.03.051

Forrest, S., Hofmayer, S. A., & Somayaji, A. (1997). Computer immunology. *Communications of the ACM, 40*(10), 88-96. http://dx.doi.org/10.1145/262793.262811

Forrester, J. W. (1961). *Industrial Dynamics*. Cambridge, MA: Massachusetts Institute of Technology Press.

Forrester, J. W. (1968). *Principles of Systems*. Cambridge, MA: Massachusetts Institute of Technology Press.

Georgiadis, P., Vlachos, D., & Iakovou, E. (2005). A system dynamics modeling framework for the strategic supply chain management of food chains. *Journal of Food Engineering, 70*(3), 351-364. http://dx.doi.org/10.1016/j.jfoodeng.2004.06.030

Han, X., & Tan, Q. (2010). Dynamical behavior of computer virus on Internet. *Applied Mathematics and Computation, 217*(6), 2520-2526. http://dx.doi.org/10.1016/j.amc.2010.07.064

Kephart, J. O., & White, S. R. (1993). Measuring and modelling computer virus prevalence. Proceedings of *1993 IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 2-15). http://dx.doi.org/10.1109/RISP.1993.287647

Khan, S., Yufeng, L., & Ahmad, A. (2009). Analysing complex behaviour of hydrological systems through a system dynamics approach. *Environmental Modelling & Software, 24*(12), 1363-1372. http://dx.doi.org/10.1016/j.envsoft.2007.06.006

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607. http://dx.doi.org/10.1016/j.im.2003.08.001

Lee, T. L., & Tunzelmann, N. (2005). A dynamic analytic approach to national innovation systems: the IC industry in Taiwan. *Research Policy, 34*(4), 425-440. http://dx.doi.org/10.1016/j.respol.2005.01.009

Mishra, B. K., & Pandey, S. K. (2011). Dynamic model of worms with vertical transmission in computer network. *Applied Mathematics and Computation, 217*(21), 8438-8446. http://dx.doi.org/10.1016/j.amc.2011.03.041

Mishra, B. K., & Pandey, S. K. (2012). Effect of anti-virus software on infectious nodes in computer network: A mathematical model. *Physics Letters A, 376*(35), 2389-2393. http://dx.doi.org/10.1016/j.physleta.2012.05.061

Murray, W. H. (1988). The application of epidemiology to computer viruses. *Computer & Security, 7*(2), 139-150. http://dx.doi.org/10.1016/0167-4048(88)90327-6

Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic dynamics and endemic states in complex networks. *Physical Review E, 63*(6), 1-8. http://dx.doi.org/10.1103/PhysRevE.63.066117

Richardson, G. P. (1996). Problems for the future of system dynamics. *System Dynamics Review, 12*(2), 141-157. http://dx.doi.org/10.1002/(SICI)1099-1727(199622)12:2<141::AID-SDR101>3.3.CO;2-F

Richardson, G. P., & Pugh, A. L. (1981). *Introduction to System Dynamics Modeling with DYNAMO*. Cambridge, MA: Massachusetts Institute of Technology Press.

Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York, NY: McGraw-Hill/Irwin.

Song, L. P., Jin, Z., Sun, G. Q., Zhang, J., & Han, X. (2011). Influence of removable devices on computer worms: Dynamic analysis and control strategies. *Computers & Mathematics with Applications, 61*(7), 1823-1829. http://dx.doi.org/10.1016/j.camwa.2011.02.010

Sung, P. C., Ku, C. Y., & Su, C. Y. (2013). Understanding Computer Virus Propagation Dynamic in Multi-perspective. *Industrial Management & Data Systems*, In Press.

Suryani, E., Chou, S. Y., Hartono, R., & Chen, C. H. (2010). Demand scenario analysis and planned capacity expansion: A system dynamics framework. *Simulation Modelling Practice and Theory, 18*(6), 732-751. http://dx.doi.org/10.1016/j.simpat.2010.01.013

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection, 2*(3), 95-109. http://dx.doi.org/10.1016/j.ijcip.2009.07.003

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198. http://dx.doi.org/10.1016/j.im.2012.04.002

Vlachos, D., Georgiadis, P., & Iakovou, E. (2007). A system dynamics model for dynamic capacity planning of remanufacturing in closed-loop supply chains. *Computers & Operations Research, 34*(2), 367-394. http://dx.doi.org/10.1016/j.cor.2005.03.005

Wolstenholme, E. F., & Coyle, R. G. (1983). The Development of System Dynamics as a Methodology for System Description and Qualitative Analysis. *Journal of Operational Research Society, 34*(7), 569-581. http://dx.doi.org/10.1057/jors.1983.137

Wolstenholme, E. F. (1994). *System Enquiry: A System Dynamics Approach*. Chichester: John Wiley & Sons.

Yuan, H., & Chen, G. (2008). Network virus-epidemic model with the point-to-group information propagation. *Applied Mathematics and Computation, 206*(1), 357-367. http://dx.doi.org/10.1016/j.amc.2008.09.025

Yuan, H., Chen, G., Wu, J., & Xiong, H. (2009). Towards controlling virus propagation in information systems with point-to-group information sharing. *Decision Support Systems, 48*(1), 57-68. http://dx.doi.org/10.1016/j.dss.2009.05.014

Yuan, H., Wu, J., & Chen, G. (2009). Infection Functions for Virus Propagation in Computer Networks: An Empirical Study. *Tsinghua Science & Technology, 14*(5), 669-676. http://dx.doi.org/10.1016/S1007-0214(09)70133-6

Yang, L. X., & Yang, X. (2012). The spread of computer viruses under the influence of removable storage devices. *Applied Mathematics and Computation, 219*(8), 3914-3922. http://dx.doi.org/10.1016/j.amc.2012.10.027

Yang, L. X., Yang, X., Zhu, Q., & Wen, L. (2013). A computer virus model with graded cure rates. *Nonlinear Analysis: Real World Applications, 14*(1), 414-422. http://dx.doi.org/10.1016/j.nonrwa.2012.07.005