

# Honeypot Protection Detection Response Recovery Model for Information Security Management Policy

Shubao Xing

Control Science, Northwestern Poly Technical University

&

Manage Science and Engineering, Xi'an Science and Technology University

Xi'an 710054, China

E-mail: xingshubao@sohu.com

Huifeng Xue

College of Automation, Northwestern Poly Technical University

Xi'an 710000, Shaanxi, China

Gang Li

Control Science, Northwestern Poly Technical University

&

Xi'an Technological University

Xi'an 710000, China

*The research is financed by Shaanxi Province Education Department: 09JK148*

## Abstract

Focusing on characteristics of information management in SME that most information security models assign the detection function to the operational process of enterprise, this paper proposes an information security management model for SMEs ---- the HPDRR (Honeypot Protection Detection Response Recovery) model. By means of empirical studies, this paper summarizes the scheme for executing, maintaining, and improving the information security management policy in SMEs in China.

**Keywords:** Small and medium-sized enterprise (SME), Information security management, Management model, HPDRR

## 1. Introduction

Information security management model is an abstract description of information security management policy. It is the base for building an information security management system. Today, based on studies on security theories, technologies, and standards, different organizations propose various information security management models. With different focuses, these models offer different ways for information security management.

Meta Group, the world largest security-issue research institute, has interviewed 7,000 specialists of technologies and security from 40 countries concerning the global information security (Ramabrahmam B V & Swaminathan G., 2005, p37-62). One of the conclusions: many interviewees agree that their companies are more vulnerable to threats in last year, or the threats are at the same level with conditions in previous year. Among these interviewees, 49% of them blame the vulnerability to threats for the absence of information security policies, 42% for the outdated IT configuration, and 26% for inadequate software patch procedures. It well illustrates the importance of information security management policy. By introducing and analyzing the famous information security management model, this paper proposes the right information security management model for SMEs.

## 2. Introduction to present information security models

### 2.1 PDRR model

PDRR (Protection Detection Response Recovery, shown in Figure 1) is a relatively mature network security model. This model consists of protection, detection, response, and recovery, forming a dynamic information security period. Each part of security policies includes a group of security unit to realize certain security functions. The first part of security management policy is protection, taking protection measures, such as patches, accessibility control, and data encryption, according to all system-known security problems. The second part of security management policy is detection. If an attacker runs through the protection system, the detection system will detect it. The function of the security front is to detect the identity of attacker, including the attack source, and system loss. Once detect an attack, the response system works, including event handling and other operations. The final front of security management policy is system recovery. It makes the system recover back to the original state after the attack.

### 2.2 PDCA model

The PDCA model is shown in figure 2. P ---- Plan: according to organizational operation requirements (include customers' and legal requirements, establish the security management scope and strategy. Confirm the objectives and ways for control by risk evaluation, including necessary process and business sustainable plan. D --- Deploy: deployment process, that is, the organization deploys information security control by following the organization's strategies, procedures, and rules, namely the selected objectives and ways for control. C --- Check: according to the strategies, objectives, and security standards, namely the legal requirements, monitor and testify the security management process and the information system security, and report the results. A --- Action: make appropriate examinations and evaluations on strategies, value the effectiveness of isms, take measures, and make continuous improvements.

### 2.3 Other model

The well-known American Internet Security System Corporation proposes the ANSM (Adaptive network security model) based on P2DR. Internet Security One takes the "life cycle" of customers' information security into consideration by analyzing technological and operational needs. It finds that seven aspects reflect the continuous circulation of information system security: plan, evaluation, design, deployment, management, urgent response, and education.

## 3. Characteristics of information security model

Due to the traits of information security threats, it is hard to identify the security incident. Meanwhile, the security incident happens quickly. An attack may last only few minutes and even shorter. SMEs have no sufficient staff for security technology. Hackers who break through the security system master technologies better than SMEs' security technologists. In the game with hackers, SMEs are often at a disadvantage. Although we can build strong security system, over time, it will face various bugs, followed by a variety of security issues. Sending warnings early against security incident and detecting it is a long-term task, full of technologies and challenges. The security staff in SMEs can not fulfill this task well. Models in this paper combine the function of detection with enterprises' operational process, which is tough for SMEs.

By visiting the small and medium-sized high-tech enterprises and information security firms in Xi'an High-Tech Development Zone, authors find what the security firms worry about is the lack of long-term attentions to information security in enterprises, that is, the long-term financial support. On one hand, it is the problem of security consciousness. On the other hand, enterprises are concerned with the endless potential investments in information security, which can not prove the benefits directly. How to establish a balance between security and benefits is a tough issue for enterprises.

Concerning information security, "to mend the fold after the sheep have been stolen" is unacceptable for enterprises, especially high-tech SMEs. Once the core technological information are destroyed or stolen, losses will be irreparable (in High-Tech Development Zone, many enterprises develop with one or two core technologies. Once losing the technological advantage, there is no base for the survival of enterprises). Therefore, early-warning and just-in-time detection of security incident is particularly important for SEMs.

## 4. Honeypot Protection Detection Response Recovery model for information security management policy

By means of wide investigations and researches, considering the situations in SMEs, this paper proposes an information security management policy model for SMEs: HPDRR (Honeypot Protection Response Recovery)

(1) The definition of honeypot: honeypot is a kind of security resource. Its values rest in being scanned, attacked,

and defeated. It means the honeypot has no real functions. Therefore, all inflow and outflow network traffic may indicate being scanned, attacked, and defeated. And the core value of honeypot is to monitor, detect, and analyze all these attacking activities.

(2) For the model periphery, that is, outside the information system, we use the real host, operating system, and applications to build a honeypot system. Because the honeypot has no real functions, it collects few data. And the collected data is from the attack of hackers. The honeypot does not depend on any complicated detection technologies, which reduces the false negative rate and false alarm rate, ensuring the high fidelity data collection. Meanwhile, the honeypot technology can collect the most advanced attack tools and methods, compensating the weak detection function of PDDR model. Most attack-detection system can merely detect the known attack according to the matched features.

The honeypot technology is right for SMEs in deployment. As an early-warning system, firstly it does not demand for powerful resources support. We can use some low-cost facilities to build a honeypot, not necessary for amounts of capital investments. Secondly, compared with other attack-detection technologies, the honeypot technology is simple. So the network managers can easily master the knowledge of attacks from hackers. The honeypot technology has some defects indeed. It needs more investments from time and energy. This job is appropriate for junior security workers in SMEs.

The honeypot locates in the periphery of the information security system of SMEs. The hacker attack is a tentative and gradual process. The honeypot is the first system attacked by a hacker. The security workers in enterprises can capture the first movement of a hacker by monitoring the data of honeypot, sending an early warning. Besides, they can judge the grade of a hacker by analyzing the traces left by the hacker in honeypot, confirming the level of early-warning.

The internal model takes references from the advantages of PDDR model and APDDR model, forming an information security period by protection, detection, response, and recovery. Here, protection can be divided into identification and authentication, access control, data integrity, data confidentiality, anti-repudiation services and components, forming a base for the security system. Detection, response, and recovery are a dynamic process. Each cycle is a process making up for security vulnerabilities, and perfecting the security management.

## 5. Empirical application

Xi'an Information Harbor Co., Ltd. builds the general network security frame based on the HPDDR model. By changing the computer network, set up the honeypot system, enhance the network access control ability, and build the information security framework. Guard the network infrastructure, local computing environment, and regional borders. Integrate the support infrastructure and achieve the necessary and proper protection in different regions. Form an in-depth protection system. After half of year operation, it achieves better operating results.

## 6. Conclusion

By means of wide investigations and researches, considering the situations in SMEs, this paper proposes an information security management policy model for SMEs: HPDDR (Honeypot Protection Response Recovery). Based on an empirical studies on HPDDR model, this paper presents the plan for applying, maintaining, and improving the information security management policy in SMEs. Finally, the paper concludes: the information management policy, mentioned in this paper, can solve the information security management issue in Chinese SMEs.

## References

- Elba U & Brian W. (2003). National review of hurricane evacuation plans and policies: a comparison and contrast of state practice. *Transportation Research Part A: Policy and Practice*, No. 37, p257-275.
- Federal Emergency Management Agency [FEMA] [OL]. (1998). Emergency Management Institute Unite 1: Introduction to ICS. Basic incident command system (ICS). *Independent Study Course*. IS-195. p1-1, 1-17.
- Jenkinsl. (2000). Selecting scenarios for environmental disaster planning. *European Operational Research*, No. 121(2), P275-286.
- Patra A K. (2006). Influence of wind speed profile and roughness parameters on the downwind extension of vulnerable zones during dispersion of toxic dense gases. *Journal of Loss Prevention in the Process Industries*, No. 19, p495-497.
- Ramabrahmam B V & Swaminathan G. (2005). Disaster management plan for chemical process industries --- Case study: investigation of release of chlorine to atmosphere. *Journal of Loss Prevention in the Process Industries*, No. 13, p37-62.

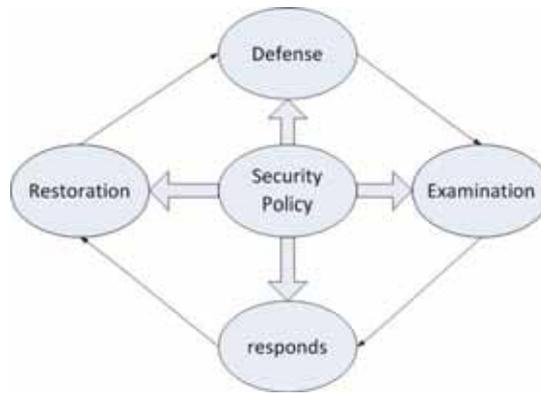


Figure 1. PDRR model

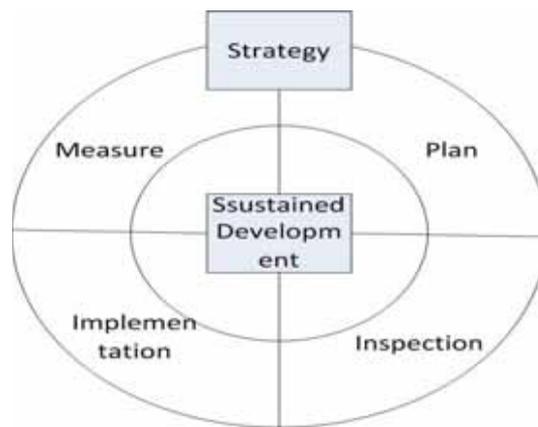


Figure 2. continuously Improved model of information security management PDCA

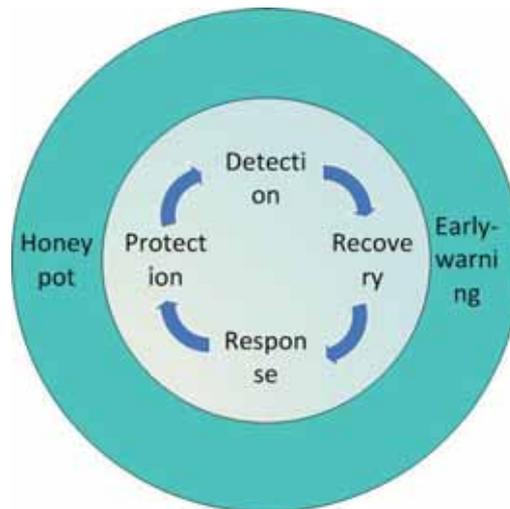


Figure 3. HPDRR Model