Case Study - SLMM Application

Tai-hoon Kim
Dept. of Multimedia, Hannam Univ., 133 Ojeong-dong, Daedeok-gu, Daejon, Korea
taihoonn@empal.com

Kouichi Sakurai
Dept. of Computer Science and Communication Engineering, Kyushu Univ., Japan
sakurai@csce.kyushu-u.ac.jp

Abstract

In this paper, application of SLMM to a case was described. Because SLMM consultants considered the target of SLMM as a virtual laboratory in commercial company, it may be difficult to say this result can be applied to real one in same way. But this case study will give enough information about the real application of SLMM to real company, and many people can understand how to modify and use SLMM according to their own environment.

Key words*: SLMM, threat level, asset level, security level*

1. Introduction and Related Information

SLMM (Security level management model) [1] was developed to maintain security level of companies and organizations. SLMM can give enough guide about security countermeasures to security officers, and by using SLMM, security officers can evaluate their security level [2, 3].

In this paper, we applied SLMM to a virtual research room in commercial company. Even though it may be difficult to say this case study can be applied to real one in same way, but this case study will give enough information about the real application of SLMM to real company, and many people can understand how to modify and use SLMM according to their own environment.

The size of commercial company describe in the case study below may not proper to be considered as real one, but it is enough to provide a guide for SLMM application. The virtual commercial company considered in this paper is a small size one, and the information related to this company is assumed as like below:

General information of company:

- The company named 'Computer Technology' was established 10 years ago, and is listed in middle standing.

- The total value of assets is about $20,000,000 USD, the total sales per year is about $50,000,000 USD, and the clear profit per year is about $5,000,000 USD.

- The average price of stock in this year is about $20 USD.

- About 200 staffs and employees are working at the department of manage, sales and AS, and research.

- A annex research institute is composed of 2 parts, and 20 researchers are working at each part.

- There are 5~6 competitors in the domestic market, and 30 competitors in the world.

- Domestic market size is about $300,000,000 USD per year, and world market size is about $5,000,000,000 billion USD.

- Total market size is extended rapidly about 10% per year.

- Recently, many large companies are preparing to be included in this market.

- Main target of SLMM is an annex research institute located in external building separately.

Business situation:

- This company threw the news that the success of new projects is coming to the public taking account stock prices.

- Because the possibility of success in the market was estimated very high, so the company got may investment proposals.

- Recently company recognized accidently that competitors organized research teams to develop similar products.

- This company decided to hire more researchers to finish the project as soon as possible and invest more money to marketing aggressively.

- Location of research institute:

- The research institute is located at the center of 6 floor in the 12 storied building.

- At each story, there are 30 research rooms, sized 900 ㎡ (30 meters long and 30 meters wide, and height is 3 meters).

- Back side of research room is blocked by double windows (a thickness of 5 mm), and the distance to nearest building is about 70 meters.

- Windows were fixed, and automatic blinds were installed.

- The wall of each research room is 15 cm cement.

- In the fore side, there is a door sized width 1.5 m and height 2 m. Door is made of wood and divided into 2 pieces.

- Wood door has a thickness of 10 cm.

- At the door, there are two locks and one smart card lock.

Inside of research room:

- In the window side, there are spaces for 2 team leaders, and their spaces are divided by partitions (a thickness of 7 cm).

- In front of the spaces for team leaders, there are spaces for 20 researchers divided by partitions.

- There is one personal computer and 19 inches LCD monitor set on the desk of each researcher.

- There are 5 server systems: 2 servers for projects management, 1 server for printer control, 1 server for DBMS, and 1 server for testing.

- There are 5 CRT monitors connected to each server.

- 2 color laser printers, 1 ink-jet color printer (combined use as like scanner and fax.) were installed.

- Wire network speed is 100Mbps, and wireless network speed is 54Mbps.

- In research room, 2 switching hubs are working.

- 1 firewall system and 1 IDS system have EAL were connected in the network.

- Anti-virus software was installed in all PCs for researchers.

- Host IDS system was installed in each server.

- Anti-virus system is updating every 1 week, and firewall system and IDS system are updating every 2 weeks.

- 64bit-base crypto technology is applied to the research room.

In/Out information of researchers:

- All researchers including team leaders are working from 9 a.m. to 6 p.m.

- All researchers including two team leaders (A and B) keep their own desk except meetings, holidays and business trips.

- Each researcher has his/her own smart card for the identification, and this card is used as a key, too.

- Each researcher has 2 keys for 2 locks.

- For emergency case, additional keys and smart card key is kept in the guardrooms.

Working information:

- Two software development projects are going on.

- One team leader and 9 researchers are assigned to each project.

- Computer systems of each researcher are in operation during working time.

- Two server systems for project management are working 24 hours.

- One server system for testing is connected to external network and working 24 hours. And some researchers connect to this server at night to check the testing status.

- One database server works 24 hours to provide some data to other system and stores testing results.

- In the morning, researchers start their work after getting data from server systems.

- Some researchers installed remote access control software in their PC to work at outside (when business trip or holiday)

Project information:

- The name of projects developed in these days are January and February.

- At least 3 years are needed to finish each project.

- Project January is in the second year development progress, and project February is in the first year development progress.

- The price of each software developed will be at least $5,000 USD per copy.

- Commercial version of each software is expected to be sold at least 10,000 copies.

- Life cycle of each commercial version is expected as 2 years.

- January is the project to development a software which can build internet shopping site automatically regardless of operating system and database management system.

- February is the project to development a software which can analyze network traffic to provide the expectation about customers' purchase. And in this software, load balancing function is included, too.

- Potential value of technology is expected at least $5,000,000 USD.

- In the market, these technologies are evaluated as upgraded one at least two or more levels

Researchers' information:

- Totally 20 researchers are working at this research room including 2 team leaders.

- Team leader A became a member of this research team after graduating university (his major is related to computer engineering) 9 years ago, and was promoted to team leader last year. There is no problem in home background and personal relationship. He is usually a man of a few words and has a strong sense of responsibility.

- Team leader B moved to this research team after working at marketing team for 8 years. Because her major was business administration, her major roles as a team leader is the analysis of user requirements and quality assurance.

- Each researcher's personal data was managed by managing department.

- All researchers joined this company after graduating university, but some researchers' major is not related to computer or programming area.

- Researcher C is a veteran programmer of 12 years career, and he was formerly a team leader at this research room (before new leader A). He has great capability in program development, but he used to miss the deadlines because he is obsessed with perfect.

- Researcher D is a programmer of 9 years career, joined this company with A together. Because D likes drinking and has very active and free character, he often makes a pleasant atmosphere.

- Researcher E is a programmer of 8 years career, he likes gambling like as a horse race and card game.

- Researcher F is a programmer of 8 years career. Because she is sometimes careless, she used to make some errors ih her source codes.

- Researcher G is a programmer of 7 years career. She is very silent, so she does not make any problem.

- Researcher H is a programmer of 7 years career, and moved to this company 3 years ago from other company. H has great capability in programming, and all his colleagues admit it.

- Researcher I is a programmer of 6 years career, and moved to this company last year because of bankrupt of his own company he established when he graduate university.

- Researcher J is a programmer of 5 years career, and has interesting to investment in stocks and funds.

- Researcher K is a programmer of 4 years career, but other researchers think K needs more career.

- Researcher L is a programmer of 4 years career, and he has no interesting to other things except the works assigned to him. He dislikes night duty and special duty.

- Researcher M is a designer of 4 years career. Because of a traffic accident, he is wearing a cast in right foot. He likes a baseball very much, sometimes makes a bet at baseball game.

- Researcher N is a designer of 4 years career. Because of a traffic accident with M together, he is wearing a cast in left arm. New baby was born a few weeks ago, so he is trying to move to other company to get more money.

- Researcher O is a tester of 3 years career. He is worrying about the shortage of time for testing.

- Researcher P is a tester of 3 years career. He manifests dissatisfaction about insufficient investment to testing environment construction.

- Researcher Q is a tester of 3 years career. He moved to this company 1 year ago because of bankrupt of former company.

- Researcher R is a tester of 2 years career. His major in university was the fine arts. But he studied computer program at a graduate school.

- Researcher S is a manual writer of 4 years career. He checks development processes always.

- Researcher T is a manual writer of 2 years career. After getting opinions from past users, she is trying to make easy manuals.

2. Security Level Decision

2.1 Definition of Threat Level

(1) Who is the potential threat agent and what is his capability?

This middle size commercial company develops and sales commercial softwares. And the security level management target is a research room located separately in the external building. Potential users of the commercial software developed by this company are other companies or people who are preparing internet based company establishment.

Potential threat agents who can attack this research room can be identified based on the [Table 4] as like:

- Nation states: It is rarely possible to apply the softwares developed in this research room to military or political areas. So it is difficult to consider nation states as the potential attacker.

- Hackers: Even though there are 5 servers and 20 PCs in this research room, there are many more easy targets in the world. So it is possible to consider well trained hacker as the attacker, but it is hard to say this hacker will attack this research room to get more computer resources.

- Terrorists/Cyber-terrorists: It is hard to say that the physical attack to destroy system or electronic attack to disable system will be forced to this research room.

- Organized crime/Other Criminal Elements: It is possible some criminals will try to steal the software from the research room and sale it to another company.

- International Press: It is hard to say that international presses have interesting to this software. If the presses want, company will provide enough information about the software to advertise it.

- Industrial Competitors: Industrial Competitors can try to steal this software to extend market share or sustain the competitive power in the market. It is possible industrial competitors buy the stolen software from criminals or cooperate with criminals to get the software.

- Disgruntled Employees: It is possible some researchers discontented with his position, promotion or salary try to steal the softwares.

- Careless or Poorly Trained Employees: Because of careless actions or conversations, some critical information related to software development project can be drained away.

Therefore, SLMM consultants can consider Organized crime/Other Criminal Elements, Industrial Competitors, Disgruntled Employees, and Careless or Poorly Trained Employees as the potential attackers.

Next stage is capability estimation of potential attackers based on [Table 5]. Some criminals can destroy or disable the research room itself, but this possibility is very low because their objective is stealing of softwares.

Because SLMM consultants can expect easily that potential attackers have capability to slip in the research room, and this means attackers can steal important information, so SLMM consultants can decide the weight for threat agent and capability identification is 3.

(2) What is the attackers' motivation?

In this case, attackers' motivation is very clear. Motivation is the steal of softwares developed in the research room. So SLMM consultants can decide the weight for attackers' motivation is 3.

(3) What is the attack type?

Potential attackers are Organized crime/Other Criminal Elements, Industrial Competitors, Disgruntled Employees, and Careless or Poorly Trained Employees.

- There is no special security countermeasure at the main door of 12 storied building (research room is 6 floor in this building). If someone wants to visit research room, security men call any researchers to notify visitors are coming. CCTV cameras are installed at main door, entrance of elevators (between 2 elevators), and the gate of each emergency staircases. Stored CCTV data deleted every 1 week, and new data are stored again. Because there is no restaurant in this building, external food service men deliver dishes to each room in the building frequently. So security men don't control their entrance. Therefore, it is possible attackers slip in the building.

- The back side of research room is walled in from behind by a wide glass; it is possible to spy upon the researchers' monitors. (Because the distance from near building is only 70 meters, highly efficient cameras can capture monitor screens. And electromagnetic signals are leaking out to outside, it is possible to restore data by analyzing these signals.

- There are two locks and one smart card lock at the door, but because all researchers have their own keys, someone may miss their keys.

- Because there is no separate space for visitors, visitors can enter to research room freely and connect to internal wireless networks. Therefore, visitors can send some internal information or data.

- There is no CCTV camera at the door, and there is no camera in the research room. So it is impossible to monitor internal researchers' action.

- Each researcher can see other researchers' monitors and works easily because the height of partitions is too low. And each researcher can check other researchers' work from the server.

- Each researcher can use domestic and international phone call freely, and the conversations by telephone do not be monitored. And each researcher can send fax messages to anyone (domestic and international) freely without any restriction. Some researchers installed and used messenger program on their own PC. All researchers have cell phone and use it freely in the room (can send MMS and photos, access to web for finding or sending information). Researchers can access internet mail system and send or receive a attachment maximum 10 megabyte. So it is possible to flow out important information.

- According to the rule, researchers' working time is from 9 a.m. to 6 p.m. but some researchers come to office at 8 a.m. and stay by 9 p.m. to do internet surfing. All researchers' PCs are connected to internet, it is possible attackers access to researchers PCs or servers passing through researchers' PCs to steal critical information.

- Some researchers are discontented with their position, omission from promotion, or wage-freeze policy. And because some researchers think their wages are too small, it is possible to yield to temptations of scout proposal and divulgement of secret.

- USB drive ports and DVD R/W are attached in each PC, and DVD disks are distributed to each researcher for back-up freely. But there is no method to control the leakage of DVD and USB from the research room.

- Some researchers installed a remote control program in their PC to work on vacation or business trip. Accesses from external terminal like this are accepted to provide work convenience.

Because there are many attack methods SLMM consultants can not expect, SLMM consultants are able to assume attackers have capability to infiltrate into research room (physically or electronically).

Important thing is that SLMM consultants identified already attackers' motivation is the steal of softwares. So SLMM consultants can expect attackers will do something actively. Therefore, weight for attack type can be decided based on [Table 9] as 5.

(4) Can attackers access to information systems?

SLMM consultants should consider about the access to information system not information itself. This is because, in these days, information is managed and stored by information systems as a digital file not the documents as like a former style.

Important information consists of many data. So even if someone may flow out the data he knows, these data are just fragments. But if someone may access information systems and find data, these can be really important data.

- Unauthorized access: If attacker accessed to information system, according to the privilege of the account cracked, attacker can obtain information. Access means not physical but electronic, so even though attacker entered into the research room, this is not mean the access if attacker can not log-on to the system.

- Establishment of unauthorized connection: A temporary unauthorized access to information system and establishment of unauthorized connection path are not same thing. The latter means attacker can access again later when he want, and will steal the information continuously.

- Disability: After steal of important information, attackers can make system disable. But because this is a proof of attack, it is very difficult to do before attackers are prepared for serious risks.

Attackers may make inroad into the research room or examine clearly the inside of the room or access to the system via networks. If the attacker is a insider, he will access to the systems directly. In any case, if attackers try to compromise information system actively with obvious motivation, riskiness will be increased.

Because enough security countermeasures are not implemented (only firewall systems, IDS, and anti-virus software), and the update cycles of these security products are too slow, attackers can establish unauthorized access channel to information system via networks.

If attackers may access to physical system directly or insiders may be changed to attackers, it will be more easy to install malicious softwares. And by using these softwares, attackers will access to information systems continuously and freely.

Therefore, the weight for access is 4 based on [Table 13].

(5) What are the tools and equipments can be used?

Performance of tools and equipments improved in proportion to price. It is a problem if someone download hacking tool from web and use it carelessly, but it will be bigger problem if someone modify this tool according to the characteristics of targets.

Fortunately, it is very difficult to optimize hacking tools and prepare expensive computer equipments, because much money and high technology will be needed to meet these requirements.

Originally tools and equipments are different things. But in these days, well trained hackers can make and control many zombies systems and then overcome the lack of high performance equipments. As a matter of course, tools and equipments do not mean the things for attacks only.

- Basic or well known: Many tools, books and knowledge sources are available already. Someone may attack the system by using these materials well known.

- Specializing: Someone may merge tools well known to make their own specialized methods, tools and equipments. And it is possible to use zombie systems to maximize the effect.

- Optimizing: Someone may modify the source code of tools and optimize it according to the characteristics of target. And they will prepare to use good and enough equipment.

Based on this classification, SLMM consultants can expect attackers may have at least specialized tools and equipments. So the weight for tools and equipments can be 4 from [Table 14].

(6) How long will the security countermeasures withstand an attack?

Information systems contain important information can be attacked, and if there may be no proper countermove, systems will be compromised.

Regardless of physical access or network access, final countermeasure about these attacks is the security mechanisms. And the total time before all security mechanisms are disabled is the 'elapsed time'. If the elapsed time is short, this means there may be no enough time to cope with the situation; otherwise long elapsed time means the security mechanisms implemented are strong enough to defend information systems.

- Because the update cycle of firewall and IDS which are protect networks of research room is too long, so it is impossible to say these systems can protect information systems well.

- Because crypto systems were established by using 64 bit, it is very hard to say this is enough to protect information systems well.

- Because some researchers did online game, messenger and investment in stocks by using their PC for business use, softwares have no relationship with research used to be installed. Therefore, it is possible malicious codes are downloaded and installed.

- Test server connected to external network has the function of bypassing security systems to provide high performance. So this test server can be in a defenseless state.

- Researchers have some problems (did not be promoted, discontented for their low salary, were in dept) may try to access information systems to steal important information.

Information systems in this research room will be elapsed in a few hours if attackers try to compromise them with modified tools and nice equipments because of weak security countermeasures. So the weight can be 5 from [Table 5].

(7) Additional weight for interrelation

There is a difference between what we can do and what we do. For example, what we can cook and what we are cooking are not same thing because the results are different. In this aspect, hackers can attack and hackers attacked are not same.

When SLMM consultants calculate the security level, after considering current environments and correlation between weight factors, they can append some more weights.

- Potential value of softwares developed in this research room may be over ten million dollars by considering market size, competition status, stock prices and research investment.

- Therefore attackers will invest millions dollars to steal these softwares.

- Attackers have clear motivation, and will prepare good tools and equipments by using enough funds. Or attackers can find assistants among the inside researchers.

- So 2 can be appended as the additional weights.

(8) Decision of threat level

From the equation (7), threat level can be decided:

Ex = 3 for threat agent and capability identification

+ 3 for attackers' motivation

+ 5 for attack type

+ 4 for access to information system

+ 4 for tools and equipments

+ 5 for elapsed time

+ 2 for correlation

= 26

Based on the total value 26, threat level can be decided as TL5 from [Table 17].

Threat level 5 has the meanings: first, attackers can destroy IS, and second, attackers can control IS.

The former one means attackers can destroy information systems itself (not only physical destruction but also electrical disability are included in this scope). And this means attackers can paralyze the whole business continuity by making information systems disable after stealing important information.

The latter one means attackers make information systems as zombie. This means attackers can control information systems freely and will steal information continuously without any problem.

In any case, TL5 means information systems are in the serious status immediate complementary measures are needed.

2.2 Definition of Asset Level

In risk management process, an estimation method of the impact of successful attack has been used. But the information SLMM consultants can provide is related to only security, so the information related to economics should be provided by economists. In other words, SLMM consultants do not evaluate the asset value or level.

It is not good idea to open whole business information to economists to evaluate asset value. And the only subject who can grasp the point about business loss is the owner of assets.

If SLMM consultants have enough knowledge about economics, there may be no problem, but it is better to get assistance from specialists to decide asset level.

Let's consider next items as the data provided by economic specialists:

- The softwares developed in this research room have similar value with annual sales of this company, and after development it is expect to wide a technical gap among competitors.

- Based on the success, it is expected the domestic market shares can be extended to about 30%, and international market shares can be extended to about 10%.

- Based on the success, it is expected this company can monopolize a market at least 1 year.

- Based on the success, it is expected stock prices go up rapidly and net profits increase to double.

- If the core technology were leaked, financial loss can be estimated as millions of dollars including 3 years' amount invested. In particular, if a competitor obtains this technology and launches similar products to the market at an early stage, this company will be at a crisis.

- Because this company is having a conference with investors after announcing the final release is near at hand, leakage of core information may break all agreements

Owners should consider all information collectively before making decision. As a matter of course, SLMM consultants are able to provide the information about security countermeasures they should implement after deciding asset levels.

Let's consider owner decided asset level after thinking next items:

- Level 1: This is a level selected when owners think the threat level is not critical and their assets can be protected by current security countermeasures, or owners think the company will not be hurt by steal of information.

But this level is not applicable to current state.

- Level 2: This is a level owners decide to invest some money to upgrade security countermeasures: security education or training for researchers, upgrade of some security products, making up for the weak points in access control.

- Level 3: This is a level owners can invest much money to upgrade security countermeasures: hiring security specialists, installing additional CCTV, attaching bio-metric access control devices, replacement of old type security products, getting a separate space for visitors, prohibition of private phone or network access, blocking of electromagnetic signal leakage, control of portable storage, changing of crypto mechanism to 128 bit base.

- To keep the assets, owners will do everything. But company is trying to hire new researchers to finish the projects on time, and advertising these new softwares on a large scale by a mass media. So now the financial state is not good enough to invest much money.

According to this basis for judgment, owners select AL3 from the [Table 18] first, and will upgrade to AL4 next time.

2.3 Definition of Security Level

Because threat level and asset level were decided, it is possible to decide security level from [Table 20]. Security level needed in this research room is SL3 as like [Table 21].

Table 1: Security Level for Research Room

Asset level	Threat Level				
	TL1	TL2	TL3	TL4	TL5
AL1	SL1	SL1	SL1	SL1	SL1
AL2	SL1	SL1	SL1	SL2	SL2
AL3	SL1	SL1	SL2	SL3	SL3
AL4	SL1	SL2	SL3	SL3	SL4

In SL3, there are two kinds of level features, one for security management part, and the other for security technology part:

Security Level 3: Quantitatively Controlled

- 3.1 Security Practices in SMP are Measured and Controlled
- 3.2 Security Practices in STP are Installed and Managed Properly

3. Selection of Security Practices

3.1 Security Management Part

SLMM consultants can summarize some possible security management practices as like next [Table 22].

Table 2: Summary of Security Management Practices

Security Area	Security Practice
Human Resource	Personnel Management
	Clearance Level
	Monitoring of Suspicious Action
	Training and Education
Operation & Administration	Establishment of Security Role
	Configuration Management of Security Controls
	Incident Identification
	Incident Management
	Monitoring of Change
	Security Control Management
	Common Use of Security Constrains and Considerations
	Guidance
	Identification of Laws, Policies, Standards, and External Influences
Physical Protection	Secure Zone
	Physical Security Perimeter Management
	Classified Materials Storing

4. SL3 Requirements

In security level 3, performance of the selected security practices should be quantitatively controlled. By collecting and analyzing the evidences of performance, organization can get the quantitative understanding of security level and an improved ability to predict performance.

This security level contains the following level features:

- Security Practices in SMP are Measured and Controlled
- Security Practices in STP are Installed and Managed Properly

To be SL3, all selected security practices should satisfy LP 3.1 and LP 3.2. To satisfy LP 3.1, all selected security practices should satisfy LR 3.1.1, LR 3.1.2, and LR 3.1.3.

And to satisfy LP 3.2, all selected security practices should satisfy LR 3.2.1. Next [Figure 3] is the summary of these things. To be SL3, 5 areas in [Figure 3] should be satisfied (1, 2, and 3 for management part, 4 and 5 for technology part).

What to satisfy of LR does not mean 100% perfect satisfaction. To satisfy LR more clearly, owners should invest additional money. So the LR is the final objective of investment, and can be satisfied gradually.

SLMM consultants should provide the information which part is not enough yet, but they can not force owners to invest their money.

LF 3.1	LR 3.1.1	1	...	...	...		
	LR 3.1.2	2	...	...	...		
	LR 3.1.3	3	...	...	...		
LF 3.2	LR 3.2.1					4	5
Level Dimension (Level Features of SL3)		SP.01.01	SP.01.02	SP.01.03	SP.01.04	SP.05.01	SP.05.02
		SA01				SA05	
		SMP				STP	
		Area Dimension - (Security Practices Selected)					

Figure 1: Security practices and level requirements

4.1 Level Feature for Management Part

Managemental level feature is applied to only SMP, and contains the following level requirements (LR):

- LR 3.1.1 Define and Perform a Standard Process
- LR 3.1.2 Coordinate Security Practices
- LR 3.1.3 Establish Measurable Goals and Manage Performance

To be SL3, all these LRs should be satisfied.

4.1.1 SP.01.01 - LR 3.1.1

Core actions to satisfy LR 3.1.1 are documentation and usage of standard process or family of processes. By documentation and standardization, staffs react in the same way about the same event.

At the former stage of documentation and standardization, reactions to the events are different and intuitive. So the consistent management is very difficult, and it is hard to expect easily how the people will react.

Security practice SP.01.01 is related to personnel management, and contains next 4 main work products.

- personnel management plan
- operational requirements specification
- hired personnel
- record of hire and retirement

There are many kinds of work products (sometimes a memo, an order or an incorporeity). Even though work product is an incorporeity, this is not a big problem. But the management will be hard, obviously.

'Record of hire and retirement' contains history of hire and retire, and 'personnel management plan' expresses where a person worked at any part, what education and training courses he passed, and what his examination mark was.

Brief record, for example, he joined the company on Dec. 1, 2008 and moved to another company on Jan. 15, 2009 can be a kind of work product. But this brief record may not give enough information about his relation to security incidents.

To meet the requirement of LR 3.1.1 for SP.01.01, whole things related to personnel management should be documented and standardized. In other words, all things mentioned in SP.01.01 should be documented, standardized, and managed.

For example, let's consider new researcher employment processes of a company.

In the processes, next things may be included: request for new researchers from research team, confirmation of finance team, announcement for new employment, evaluation from management team, education and training for new researchers, work assignment to new researchers, and so on. These all processes should be documented, standardized, and managed.

By checking all information about researcher (where a researcher worked, what his characteristics are, what his interesting is, what his work is, and so on), it is possible to predict potential security incidents related to this person.

4.1.2 SP.01.01 - LR 3.1.2

Core actions to satisfy LR 3.1.2 are the coordination of activities throughout the organization. Many significant activities are performed by disparate groups within the organization and cooperative groups of outside organizations, therefore, a lack of coordination can cause delays or incomparable results. Thus the coordination of intra-group, inter-group, and external activities should be addressed.

To meet the requirement of LR 3.1.2 for SP.01.01, communication among the various groups within the organization and communication with external groups should be coordinated.

Because the focus is related to personnel management, the coordination of intra-group, inter-group, and external activities for personnel management should be addressed. If it is enough to meet the requirement of LR 3.1.2 only, any kind of coordination is acceptable, for example, oral contract or agreement is possible.

But as previously stated, to meet the requirements of LR 3.1.1, all things related to personal management should be documented, standardized, and managed. To meet the requirements of LR 3.1.1 and LR 3.1.2 together, communication among the various groups within the organization and communication with external groups for personnel management should be documented, standardized, and managed, too.

Let's consider new researcher employment processes again.

In the employment processes, many kinds of coordination of intra-group, inter-group, and external activities should be addressed: coordination between research team and finance team, coordination between advertising team and finance team, coordination among training team, research team, finance team, external review team, and external education team, and so on.

And all these things should be documented, standardized, and managed, too.

4.1.3 SP.01.01 - LR 3.1.3

Core actions to satisfy LR 3.1.3 are establishment of measurable goals for the work products and taking of corrective action as appropriate.

It is possible to evaluate and correct objectives only in the case of using quantitative objectives. So the objective "all researchers should get CISA certificate" is better than "all researchers should have enough knowledge about security". And to achieve objectives, standard processes can be modified.

Let's consider new researcher employment processes again.

To meet the requirements of LR 3.1.1, LR 3.1.2, and LR 3.1.3 together, for example, it is possible to make objective as like: Based on the documented and standardized process, training team, research team, finance team, external review team, and external education team should cooperate to make all researchers can get CISA certificate in 1 year.

This is an example. So SLMM consultants should provide proper guidelines by considering environments of the company.

4.2 Level Feature for Technology Part

This level feature related to technology contains only one level requirement (LR):

- LR 3.2.1 Install and manage security technology requirements

To meet the technical requirements of SL3, only LR 3.2.1 should be satisfied.

Because 2 security practices (key length and key management) were selected, next requirements should be satisfied.

- Key length:

  - Public Key 1,568 bits

  - Shared key 90 bits

- Key Management:

  - SMI Cat Y

  - 160+ exponent 1,024+ modulus public key length,

  - 160+ hash key length

5. Conclusion

In this case study, small size research room was considered to apply SLMM. All information related to research room, researchers and projects developed are assumed, and general level security countermeasures were assumed, too. But to apply SLMM to real company, more detail information should be checked.

In this case study, only basic information was considered to decide threat level. To decide real threat level, all information from personnel to whole systems should be checked.

Asset level definition should be done by owners. SLMM consultants should provide threat information to owners, and after getting the result of asset level from owners, decide security level with owners together.

After deciding security level, SAs and SPs should be selected. It is not good idea to select too many SPs. To implement SP, owners should invest much money. So SLMM consultants provide enough information to owners to select proper SPs (Owners can append more SPs later).

After deciding security practices, LPs should be implemented. Because each LP is described as a general purpose thing, SLMM consultant should modify it.

Most important thing is continuous management. Because many factors in security environment are changed continuously, threat level and asset level will be changed. Therefore, security level should be managed continuously.

References

[1] Tai-Hoon Kim, Gil-cheol Park and Kouichi Sakurai: A study on Security Level Management Model Description. International Journal of Multimedia and Ubiquitous Engineering, Vol.3 No.1 January 2008, pp.87-96

[2] Tai-Hoon Kim, Seok-soo Kim and Kouichi Sakurai: Definition of Security Practices for Security Level Management Model. International Journal of Security and Its Applications, Vol.2, No.1, January 2008, pp.63-72

[3] Tai-Hoon Kim and Kouichi Sakurai: A Study on Security Level Features and Level Requirements in Security Level Management Model. International Journal of Software Engineering and Its Applications, Vol.2, No.1, January 2008, pp.109-118