EQST insight

Analyzing risks and deriving improvements through cases of cyber infringement incidents

Lee Min-ju, Hi-TECH1 DEPARTMENT Manager

■ Outline

Today's business organizations are gradually moving away from analog to a digital environment due to the development of the industrial environment, increasing the companies' digital dependence. These environmental changes are causing many infringement incidents and we often hear about related incidents, especially through media reports.

The proverb 'Lock the stable door after the horse is stolen' is used ex post facto to mean 'after losing something important, you learn its value and only then do you pay attention and try to make up for it.' Looking at this from the perspective of an information security officer, several lessons and expected benefits can be drawn.

First, it can be seen that advance preparation and prevention are needed, i.e. establishment of appropriate security systems and procedures in advance, rather than strengthening security measures after a security incident occurs. In addition, it is important to recognize that locking the stable door should not be one-off but regular maintenance, and response plans must be prepared periodically when new security threats or technical vulnerabilities are discovered. Lastly, it can be seen that it is necessary to determine the cause, i.e. how the horse was stolen, and there must be a comprehensive security strategy for preventing similar incidents from occurring again, including security policies, processes, and response.

To this end, first, you must have insight into current security trends and new threats. You can get this insight through a critical approach to news of infringement incidents. In this headline, we would like to introduce a strategy for diagnosing organizational risks and deriving improvements through cases of cyber infringement incidents as a way to take a critical approach.

■ Lessons learned from the cases of infringement incidents

The following lessons can be learned from the cases of infringement incidents:

① Past infringement incidents enable early response to the latest security threats.

② Risk prediction

③ Improved ability to respond

④ Security update

⑤ Risk assessment and vulnerability management

⑥ Analysis of security industry trends

■ The need to manage information fatigue

Recently, cyber infringement incidents have been occurring constantly, and the amount and complexity of information can be said to have a significant impact on individuals and organizations. Moreover, as technical terms and concepts of cyber security change and develop day by day, information fatigue is also significant.

Major cyber threats of 2023 (part)
An attack impersonating a domestic portal site turns out to be performed by APT masterminded by North Korea.
The Kimsuky group was pointed out as the mastermind behind the hacking of broadcasting companies and general companies.
The Clop Ransomware Group's campaign that exploited the Goanywhere vulnerability
The Mustang Panda group's attack against European companies
The Chinese APT group's attack targets a company developing data loss prevention software in East Asia
The supply chain attack, which exploited the 3CX program, targeted a Taiwanese PC company.
The RedHotel group attacked a Taiwanese semiconductor company.

From the perspective of those in charge of collecting and processing cyber threat trends, measures are needed to manage and relieve information fatigue. In addition, measures to effectively manage information must be prepared to increase work efficiency.

■ Setting information priority

As a way to reduce information fatigue among various kinds of news about incidents, you must classify infringement incident information and set the priority of information as shown in the table below.

Through this classification and priority setting, persons in charge can focus on important information, respond quickly to urgent situations, and thus effectively reduce information fatigue.

Classification of infringement incidents information		
Suitability	**Timeliness**	**Accuracy**
Is it relevant to us?	Do you need an immediate response?	Have the facts been checked?

① Suitability: Compare the impact of incident information on the industry and determine whether it is a threat to the organization

② Timeliness: Is it happening now? Determine whether there is a need to diagnose the organization through quick response

③ Accuracy: Is the collected information accurate?

Data processing procedure	
Stage	**Description**
Intelligence	Data that has not been verified or evaluated
Information	Data validated through the analysis and evaluation process
Knowledge	Data that can be utilized as general contents and information are aggregated

① Intelligence: intelligence data collected through various channels (examples: CyberTrace Threat Intelligence, and OSINT)

② Information: data reported as intelligence, security incident news, processed data released by security companies, etc.

③ Knowledge: data reports in a format that our organization can utilize through intelligence+information

■ Example of using other incident cases

The following is a storytelling-based case that quotes the proverb, 'Lock the stable door after the horse is stolen.' Depending on the environment and manpower of each organization, infringement incidents can be organized in various forms, but if analyzed based on the classification of the information on infringement incidents and data processing standards described above, it can be used as a sufficient basis to explain the importance of checking the vulnerability of the internal environment.

Case 1.

Organization A is a company that builds and operates a barn using state-of-the-art facilities and is in competition with Barn B located in a neighboring village. We recently received information from a feed company that visited the barn, and obtained the intelligence that an unknown criminal broke into Barn B. We confirmed that a thief entered the barn and stole the cattle.

Classification of infringement incident information		
Suitability	**Timeliness**	**Accuracy**
Is it relevant to us?	Do you need an immediate response?	Have the facts been checked?
Companies in the same industry	A livestock farm system that	Check for property damage

Stage		**Storytelling**	**Response from the viewpoint of information security**
1	**Intelligence**	Climbing over the wall of the livestock farm.	Is this an intrusion through the backdoor?
		Through the door of the farm	Is access privilege managed properly?
		Disabling the alarm system	Are detection policies and logs managed properly?
2	**Information**	Climbing over the low wall, disabling the security system with tools, and opening the door to exit	Checking whether an attacker can easily infiltrate the internal system Checking the route through which the tools used by the attacker can be brought in Checking the behavior of the unauthorized attacker, i.e. accessing the security system and deleting logs or evading the detection policy
3	**Knowledge**	Identifying the attacker based on the information on the tool used by the attacker, and checking the height of the wall, and the security policy related to the security system	1) Profiling the attack group through indicator of compromise 2) Checking traces with regard to indicator of compromise 3) Performing simulation of the attack using security equipment 4) determining the impact 5) Preventing incidents by managing privileges, and identifying logs of unauthorized requests and access by unauthorized users

■ How to use security incident case study

Several methodologies and models have been developed to more efficiently organize various kinds of security incident intelligence. Below, we will introduce an easy-to-visualize method using actual examples.

1. Diamond model: A conceptual framework used to analyze and understand cyber attacks.
   A. Threatening activity analysis: Identifying the threatening activity of the subject performing the attack and indicating the motivations and goals of various threatening activity subjects such as individuals, cyber crime organizations, and national agencies.

   B. Tactics: As tactics describe the methods and techniques used by the threatening activity subject to carry out the attack, visualize the response to the attack tactics used by the attacker

   C. Objective: It means the purpose of the attack carried out by the threatening activity subject (information leakage, financial gain, malicious actions against competitors, expansion of political influence, etc.)

   D. Infrastructure: Infrastructure refers to various resources and tools used by the threatening activity subject for attacks (indicator of compromise, malicious software distribution, supply chain attack management system, anonymous proxy server, etc.)

2. Expected benefits of the diamond model
   A. Threat monitoring: It is possible to monitor the tactics of cyber crime organizations and attackers and attack attempts for various purposes, and manage attack patterns and trends.

   B. Risk assessment: Through incident trends, the vulnerability of the organization and the possibility of attacks by threat activity subjects can be confirmed and reduced in advance.

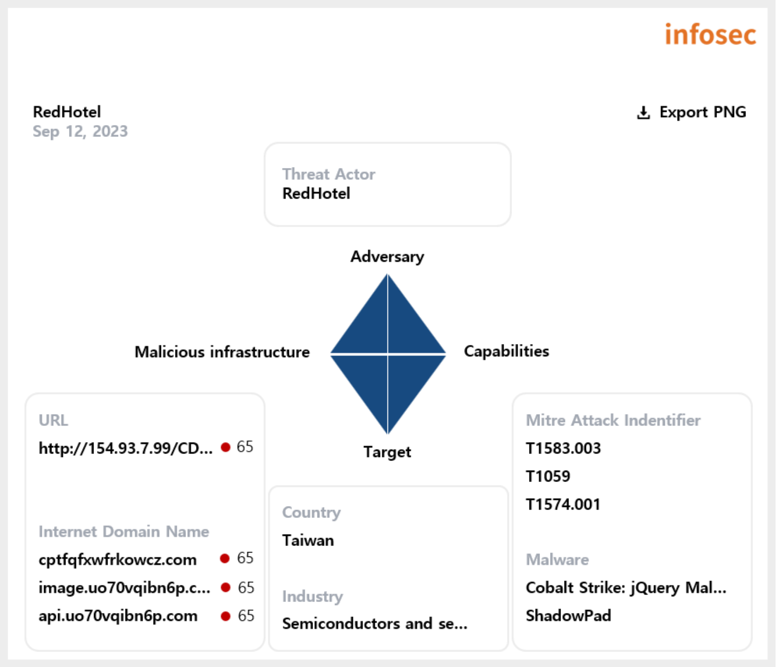
   C. Response strategy development: It is possible to provide insight into cyber threat response strategies and develop and strengthen the organization's information protection and response plan.

   D. Information sharing: It is possible to build an effective cyber security ecosystem by encouraging information sharing and cooperation.

The following case is an actual cyber infringement incident that targeted the industry group to which clients belonged. The impact of the threat information that occurred in this incident was checked based on the diamond model, and the security data was visualized.

Case 2.
China-linked cyber spies backdoor semiconductor firms with Cobalt Strike (actual article October 5, 2023)

Classification of infringement incident information		
Suitability	**Timeliness**	**Accuracy**
Is it relevant to us?	Do you need an immediate response?	Have the facts been checked?
Companies in the same industry	Urgent response to the client's competitor	What was confirmed through news reports

Stage		**Provision of information**	**Diamond model**
1	Intelligence	News articles, CTI companies	 infosec RedHotel Sep 12, 2023 Export PNG Threat Actor RedHotel Adversary Malicious infrastructure Capabilities Target URL http://154.93.7.99/CD... ● 65 Internet Domain Name cptfqfxwfrkowcz.com ● 65 image.uo70vqibn6p.c... ● 65 api.uo70vqibn6p.com ● 65 Country Taiwan Industry Semiconductors and se... Mitre Attack Indentifier T1583.003 T1059 T1574.001 Malware Cobalt Strike: jQuery Mal... ShadowPad
2	information	CTI Intelligence Report	
3	Knowledge	Replace it with data visualization	

Source: Reprocessing of the image provided by Recorded Future (CTI company)

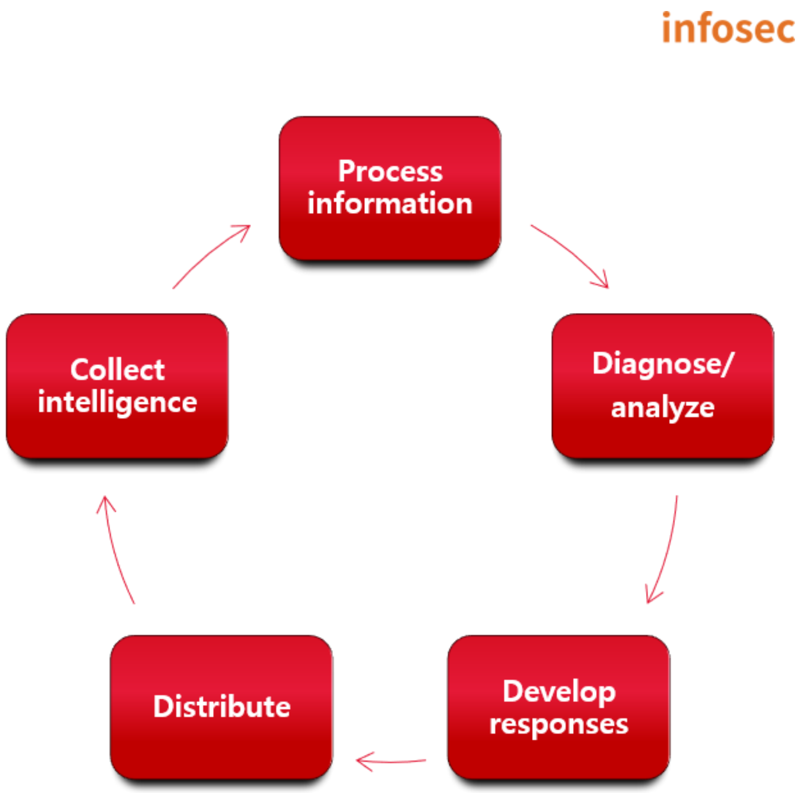
The response plan based on each item of the diamond model can be divided into the following items:

Item	Description	Things to check
Adversary	The RedHotel attack group believed to be supported by the Chinese government	- Latest attack group trends - Registering attack group monitoring target
Malicious Infrastructure	Infringement metrics exploited in attacks	- Inspecting the internal system through indicator of compromise - Blocking indicators of compromise in advance
Capabilities	Information on attack methods/paths using attack tactics and strategies through the miter attack framework	- Developing kill chain strategies for attack tactics and strategies - Developing security system detection - Investigating traces of infringement

If you use this model, you will be able to visualize and manage incident trends, and connect trend information with an understanding of the tactics and procedures used by the attacker.

■ Effective management of incident trends

It is important to identify many accident trends and generate data, but in order to manage accident trends meaningfully, incident trends must be managed in a circular manner, e.g., learning from other organizations' accident trends and preparing for incidents that may occur in the future.



1. Collect intelligence: Obtain infringement incident information from various information sources and establish a security system inspection plan.

2. Process information: Process data so that collected intelligence data can be converted into information.

3. Diagnose/Analyze: ① Develop a kill chain plan and diagnose the internal system for contents identified through intelligence + information processing ② Develop a diagnostic plan and detection plan by summarizing tactics and technical procedures

4. Develop responses: Organize information obtained through diagnosis/analysis

5. Distribute: Spread information, including improvements and recommendations, to relevant departments and people in charge.

■ Closing

In order to diagnose your organization in an environment where various incidents occur, it is important to analyze external threats, derive improvements, and make progress. There are various forecasting methodologies to do this, but all processes begin with ‘interest’. Therefore, we hope that information security managers first pay attention to various infringement incident cases and diagnose the organization's risks and find areas for improvement through the infringement incident analysis method introduced in this headline.

SK Shieldus provides comprehensive consulting necessary for corporate cybersecurity risk diagnosis based on our accumulated know-how and proprietary skills. We have the largest professional workforce and human capabilities in the industry, and we built and implement information security consulting methodologies in various fields such as security consulting, ransomware response service, hacking incident analysis, penetration testing, and vulnerability diagnosis, and deliver optimized solutions to various companies.

We hope that through SK Shieldus’ consulting, we will be able to respond effectively and systematically to cyberattacks that are becoming more intelligent day by day. For more information, please visit the official blog of SK Shieldus.