HOW TO SELECT A CONSULTANT — PART 3

Hiroyuki Watanabe: NEC Corporation
Tokyo JAPAN

ABSTRACT

In part two of this white paper, the author introduced the basics of “Zero Trust.” In part three of this paper, the author dives deeper into the practice of mitigating the effects of a cyber-attack.

INTRODUCTION -PROCEDURE

The author outlines the top-level procedure once in mitigating a cyber breach:

(a) Eliminate the sense of weakness in information system security.

(b) Make people in your company aware that technical knowledge is much more important than general knowledge of information system security.

(c) Make them aware that cyber criminals don’t like to take measures that don’t cost the system (make them aware of the importance of management).

(d) Define a comprehensive categorization of resources by impact magnitude.

Start with the resources with the highest impact. Is there a keen awareness of any obstacles that have yet been identified? Does the management of the company need to hire outside consultants to solve the problem?

For purposes of this paper, the author would like to introduce a more specific method (d) that will serve as a guideline to build relationships with outside consultants and provide confidence in the relationship.

DEFINE THE PROBLEM

The key issue with cyber-attacks is to eliminate the anxiety of those in the field and in management based on the awareness that they are not security professionals, to reaffirm the importance of what they should do themselves, and to give them the confidence to do it, thereby preventing the failure to rely on outside consultants to the extent necessary.

There is a tendency to try to rely on consultants from the beginning and fail because of insecurity based on the perception that “we are not security experts,” misleading management into believing that engineers in the field do not have sufficient skills.

As explained in the previous paper, the relationship between factory resources and impact is not something that external consultants can understand. In some cases, the consultant may end up disclosing “confidential internal company trade secrets that are prohibited from being disclosed outside the company. Perhaps you might follow the consultant’s recommendation and focus only on complying with regulations, making only excuses to the public and not following essential safety protocols. In the worst case, you may end up spending a lot of money to upgrade company infrastructure before any substantive measures have been considered in order to secure the consulting firm’s most recent profit. While infrastructure reinforcement is necessary in the big picture, implementing it before the resource extraction and compartmentalization design described in (d) can be done may result in waste, and may be an excessive investment in terms of the overall business.

Therefore, it is very important that the field engineer, as well as management, have confidence at the specific procedural level and have an appropriate relationship with the consultant.

PROBLEM RESOLUTION-GETTING TO THE ROOT CAUSE

In the procedure outlined in the previous paper, the following steps are indicated as how one should proceed in response to defining a comprehensive categorization of resources by magnitude of impact.

The following are some specific steps that you should take to:

i) Classify what people, what data, what equipment, what materials are involved in product manufacturing and how much they affect the business.

ii) Consider a draft compartment definition (draft operating rules) to minimize the scope of impact in case of an attack (In the case of humans, we think they've been bought off).

Specifically, we will show two ways to proceed: One is to proceed by analogy with the story, and the other is to proceed in light of the BUSINESS CONTINUITY PLAN for natural disaster response.

This section also explains how to establish such a relationship with a consultant after comprehensively classifying resources by impact from a businesscontinuity perspective and designing the parcel.

Of course, if a consultant who makes heavy proposals for network infrastructure reinforcement, etc. while skipping the process of comprehensively classifying resources by impact and designing the parcel from a business continuity perspective, we should decline the proposal at that point.

To dispel concerns based on the realization that we are not security professionals, let's consider a story from a time when there was no IT, no IP networks, and no firewalls.

A STORY FROM THE PAST

Once upon a time, in an era when hunting and gathering had replaced a life of mainly farming, there was a village called Utaka. The village had a sacred treasure that brought rain, and every year there was a bountiful harvest, even when other villages had bad harvests. However, in an era when a new culture was coming from a large country across the sea, a new weapon and its manufacturing method were introduced to the neighboring villages.

Taking advantage of this weapon, the village of Nimu began to raid neighboring villages in years of crop failure. Nimu then discovered the existence of Utaka's rain-calling sacred treasure. Utaka had to defend its rain-calling sacred treasure from Nimu's attacks.

Nimu obtained the password to get through the village gate by bribes, broke in, overheard what the village elders were saying, and learned of the existence of the sacred treasure. Utaka also heard rumors that Nimu had obtained the secret and began to consider measures to protect the harvest, the sacred treasure and the lives of the villagers.

At first, we came up with unrealistic ideas such as asking a country across the sea for new weapon manufacturing methods, or building deep dugouts and high fences, but we had neither the manpower nor the time frame to do so. Realizing that a perfect defense was not possible, we decided to minimize the damage caused by the attack and restore life to normal as quickly as possible after the attack.

What are the things in the village that need to be protected?” → ”Fields,” “family,” “villagers,” “food in the storehouse,” “ sacred treasure…”

In the midst of all this, “what will it take for the village to remain prosperous in the years to come?” → If we had “sacred treasure” and “villagers,” we would be able to survive with a bountiful harvest next year and the year after that.

We decided where to place the most important items in the multiple compartments, and determined how to protect and monitor them based on their importance and degree of impact. They also decided on how to strengthen the operational methods. To allow villagers working in the fields to escape to safer areas, the shelters in the living area were deepened and fortified with the strongest defenses, and surveillance was strengthened by dividing the area into multiple compartments. Crops were placed in fenced-off, high-bay warehouses, but the worst-case scenario was that they would have to be ingested. The sacred treasure was already stolen and Faked so that it no longer existed. Of course, the password has been reinforced to change periodically. Now, as you are probably aware, it doesn’t matter if you have IT, an IP network, or a firewall, you can still consider factory security by contrasting it with a story. No need to be afraid anymore, no need to lose confidence. Let’s get on with it.

Step 1: Gather and organize the information needed to determine security measures

At Utaka, when deciding how to prepare for Nimu, we initially had only unrealistic ideas with insufficient people and time, but by analyzing and organizing the items to be protected, their importance, uneven zones, and threats, we were able to finalize our security measures. Before considering security measures in a factory, it is necessary to analyze and organize information such as requirements from stakeholders and the supply chain; external requirements such as compliance with laws, standards, and guidelines; internal requirements such as management policies and the current state of security; and the objects to be protected. This information needs to be analyzed and organized.

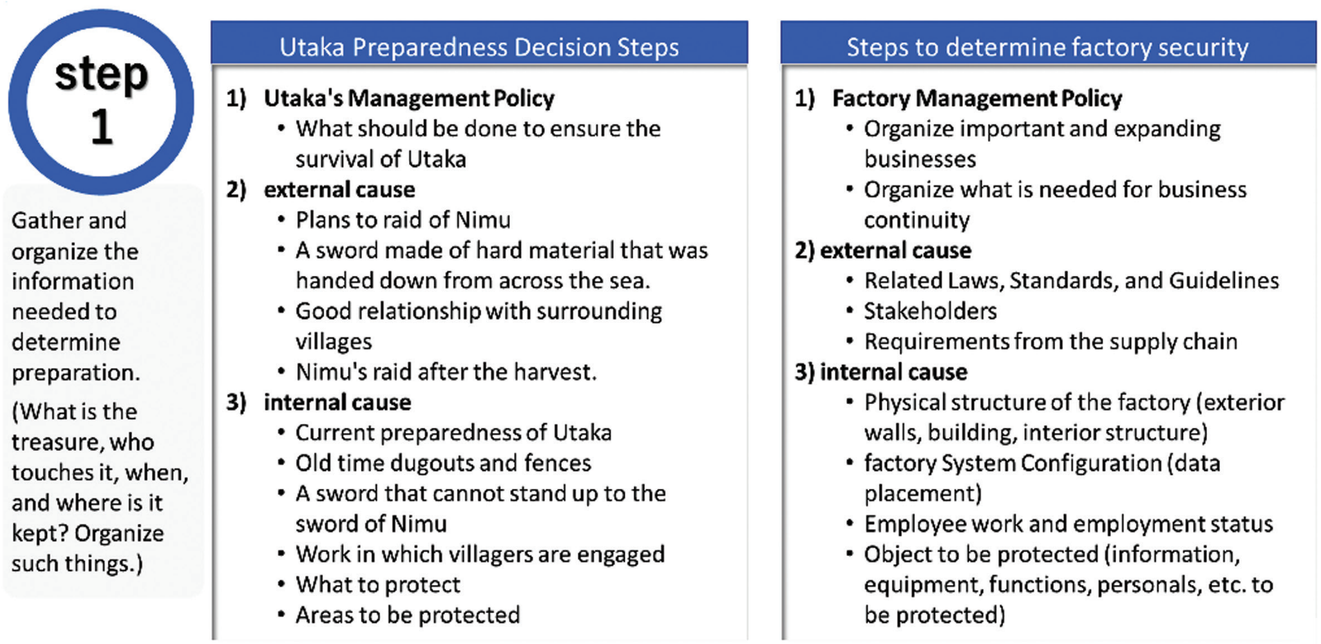
Step 2: Planning security measures

In Utaka, based on the information in Step 1, the company first decided on a policy for preparing for Nimu, such as protecting the fields, giving up the fields if they are invaded, and focusing on areas where people live, and then decided on specific measures to be taken. In factories, factories also need to agree on security measures at the policy level, taking into account external requirements and internal factors such as the conditions of the factory and the cost that can be spent on security, and then formulate specific security measures.

Step 3: Implement a PDCA (Plan-Do-Check-Act) cycle for security measures

Utaka repeats Step 1, Step 2, and Step 3 by evaluating and analyzing the battle after implementing the security measures established in Step 2, although this explanation is omitted in the above description of the story. Of course, factories need to repeat Step 1, Step 2, and Step 3 and continuously evolve them in response to changes in the factory environment, technological advances, and other factors.

Fig. 3.1.2-1 Step 1: Collect and organize information necessary to determine security measures



step 1

Gather and organize the information needed to determine preparation.

(What is the treasure, who touches it, when, and where is it kept? Organize such things.)

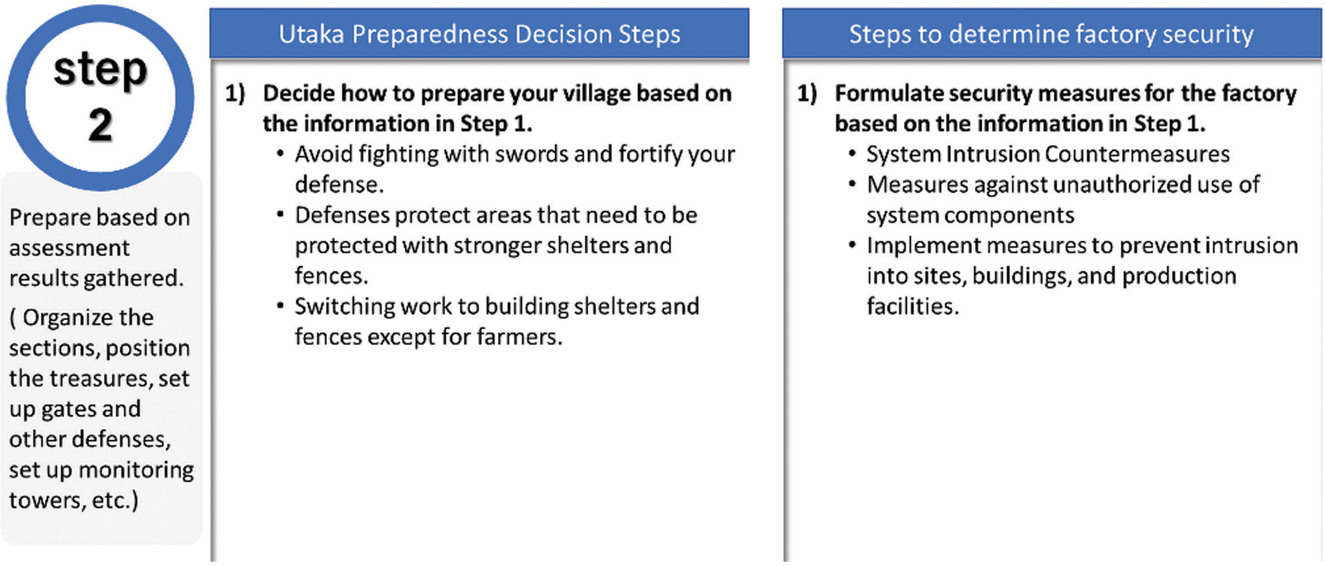
Utaka Preparedness Decision Steps

1) **Utaka's Management Policy**
   - What should be done to ensure the survival of Utaka
2) **external cause**
   - Plans to raid of Nimu
   - A sword made of hard material that was handed down from across the sea.
   - Good relationship with surrounding villages
   - Nimu's raid after the harvest.
3) **internal cause**
   - Current preparedness of Utaka
   - Old time dugouts and fences
   - A sword that cannot stand up to the sword of Nimu
   - Work in which villagers are engaged
   - What to protect
   - Areas to be protected

Steps to determine factory security

1) **Factory Management Policy**
   - Organize important and expanding businesses
   - Organize what is needed for business continuity
2) **external cause**
   - Related Laws, Standards, and Guidelines
   - Stakeholders
   - Requirements from the supply chain
3) **internal cause**
   - Physical structure of the factory (exterior walls, building, interior structure)
   - factory System Configuration (data placement)
   - Employee work and employment status
   - Object to be protected (information, equipment, functions, personals, etc. to be protected)

Fig. 3.1.2-2 Step 2: Planning security measures



step 2

Prepare based on assessment results gathered.

(Organize the sections, position the treasures, set up gates and other defenses, set up monitoring towers, etc.)

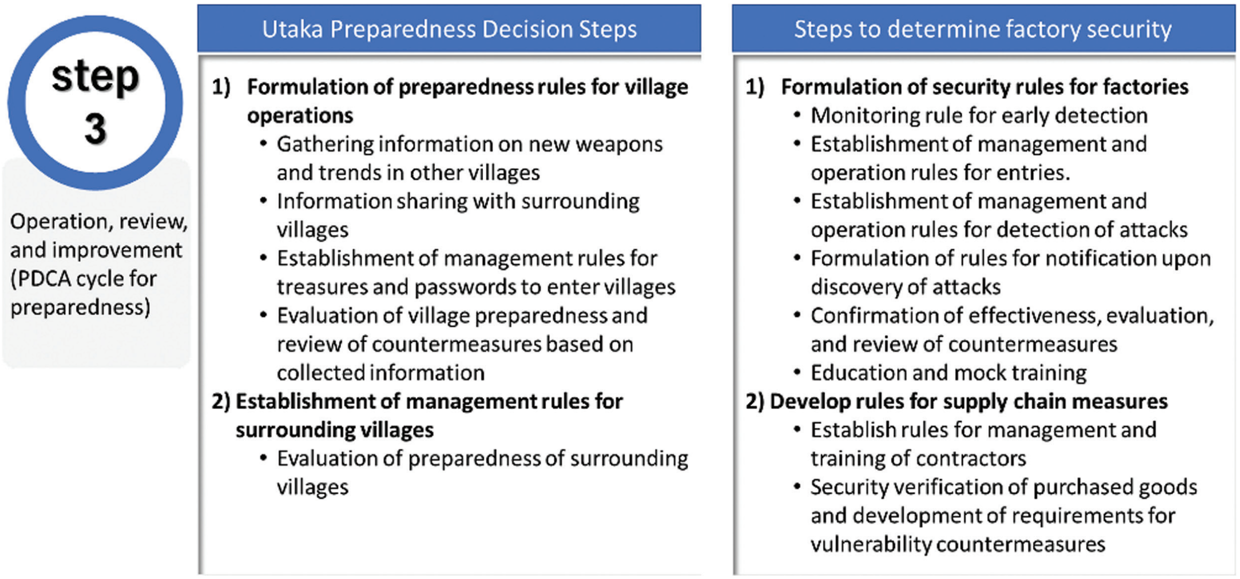
Utaka Preparedness Decision Steps

1) **Decide how to prepare your village based on the information in Step 1.**
   - Avoid fighting with swords and fortify your defense.
   - Defenses protect areas that need to be protected with stronger shelters and fences.
   - Switching work to building shelters and fences except for farmers.

Steps to determine factory security

1) **Formulate security measures for the factory based on the information in Step 1.**
   - System Intrusion Countermeasures
   - Measures against unauthorized use of system components
   - Implement measures to prevent intrusion into sites, buildings, and production facilities.

Fig. 3.1.2-3 Step 3: Implement PDCA Cycle for Security Measures



step 3

Operation, review, and improvement (PDCA cycle for preparedness)

Utaka Preparedness Decision Steps

1) **Formulation of preparedness rules for village operations**
   - Gathering information on new weapons and trends in other villages
   - Information sharing with surrounding villages
   - Establishment of management rules for treasures and passwords to enter villages
   - Evaluation of village preparedness and review of countermeasures based on collected information

2) **Establishment of management rules for surrounding villages**
   - Evaluation of preparedness of surrounding villages

Steps to determine factory security

1) **Formulation of security rules for factories**
   - Monitoring rule for early detection
   - Establishment of management and operation rules for entries.
   - Establishment of management and operation rules for detection of attacks
   - Formulation of rules for notification upon discovery of attacks
   - Confirmation of effectiveness, evaluation, and review of countermeasures
   - Education and mock training

2) **Develop rules for supply chain measures**
   - Establish rules for management and training of contractors
   - Security verification of purchased goods and development of requirements for vulnerability countermeasures

HOW TO PROCEED WHEN A NATURAL DISASTER OCCURS?

BUSINESS CONTINUITY PLAN (BCP): As we have explained in this white paper series, security measures have shifted from defense to business continuity, so it is only natural that factories should proceed with reference to the natural disaster response BCP they have prepared thus far.

(1) How to prepare to minimize damage (disaster mitigation)

(2)How to recover quickly (early recovery)

It is exactly the same concept, so rather than losing confidence, we can proceed as if we are good at what we do. In fact, at our factory, we were able to promote our initiatives with confidence, saying, “This is just like our BCP for natural disasters! and the factory was able to promote the initiatives with confidence. The way to proceed is the same as in the BCP for natural disasters: “Each plant creates its own rules, prepares, operates, and trains its own staff.

Disaster BCP and cyber-attack response BCP have a common flow.

1. Detection ~ Escalation
2. Identification of the extent of damage
3. Consideration of alternatives
4. Plant/production line operation decisions
5. Reporting to Customers and Stakeholders
6. End of task force
7. Education and Training
8. advance preparation

DIFFERENCES BETWEEN BCP FOR NATURAL DISASTERS AND BCP FOR CYBER-ATTACKS THAT SHOULD BE NOTED

I have already explained this in the second paper in the series, but I will restate it.

What makes it different from a natural disaster is that (A It is not visible when it occurs, and (B) Smaller parcels to be separated to minimize the sphere of influence.

(A) It is not visible when it occurs.

It is essential to have a monitoring method to detect the occurrence of an outbreak. In many cases, there are no clear criteria for determining the occurrence of an incident, so it is important to decide in advance under what conditions an incident will be determined to have occurred, or the initial response will be delayed, making it impossible to minimize the impact on the business and achieve early recovery. It is also important to make technical preparations, such as determining how many terminals onsite at the same time are abnormally slow to determine that an intrusion has occurred and to determine whether or not to activate the BUSINESS CONTINUITY PLAN.

More importantly, unlike natural disasters, human beings have to make the final decision on the occurrence of outbreaks that affect the business, such as the suspension of shipments. This decision cannot be made on the factory floor, so it is necessary to decide who in the management team will make the decision. And if the conditions for this decision are inadequate or the speed of the decision is too slow, management should be made aware that this will result in a loss of trust from customers and the public, and damage to future business operations. Since you cannot invest and prepare for costs that are not commensurate with the size of your business, this will allow management to recognize this as a problem for which they are directly responsible for the first time and to be in a position to worry about it with you.

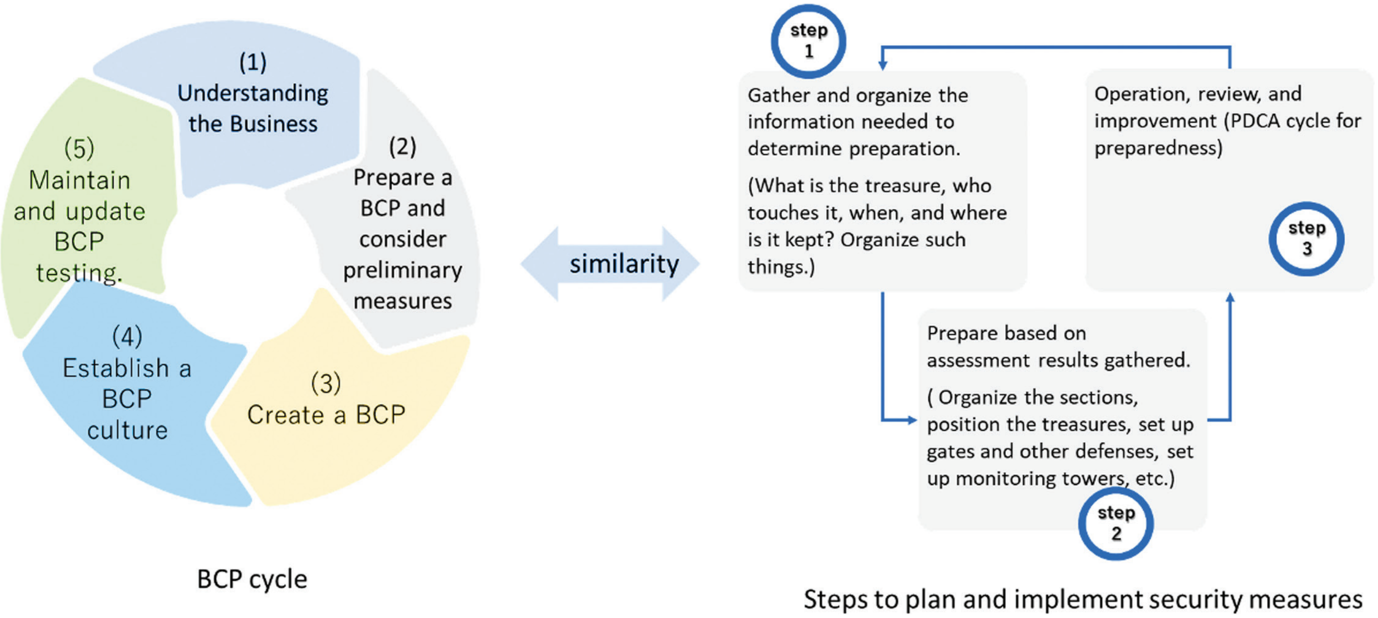
(B) Smaller parcels to be separated to minimize the sphere of influence.

In the BCP for natural disaster response, the size of the separation compartment has been considered based on the assumed impact area of a single natural disaster. For example, we have probably distributed parts supply routes to different regions, or distributed data backup to different regions. However, since cyber-attacks are targeted with pinpoint accuracy, the size of separation compartments is classified by the degree of impact on business continuity in the event of an attack, and separation compartments are defined in units that are convenient for controlling access to that resource.

For example, “Assuming that a measuring instrument that measures the quality of products shipped from a factory is attacked, design the separation compartment with considerations such as “prohibit the flexibility of the measuring instrument within the factory, bundle it in the shipping line, and separate the range of connections that can be made.

The compartment definition is an operational rule, so it can be designed on the factory floor. IT and security technologies are needed only after the actual construction of the compartment. Therefore, it is recommended that the compartment definition be implemented on the factory floor, and only after the compartment is actually created should it be outsourced to a consultant or IT/security service provider.

Fig. 3.2.2-1 Cycle of Natural Disaster Response



(1) Understanding the Business

(2) Prepare a BCP and consider preliminary measures

(3) Create a BCP

(4) Establish a BCP culture

(5) Maintain and update BCP testing.

similarity

step 1

Gather and organize the information needed to determine preparation.

(What is the treasure, who touches it, when, and where is it kept? Organize such things.)

step 2

Prepare based on assessment results gathered.

(Organize the sections, position the treasures, set up gates and other defenses, set up monitoring towers, etc.)

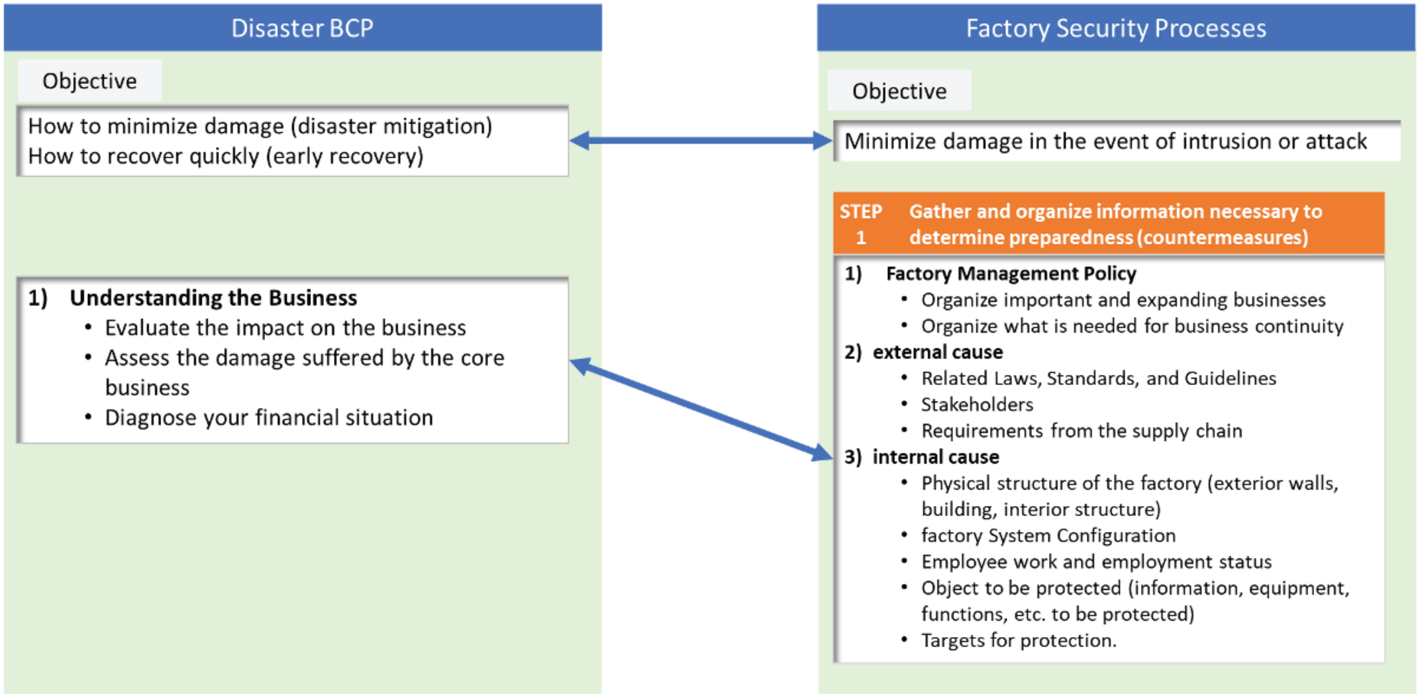
step 3

Operation, review, and improvement (PDCA cycle for preparedness)

BCP cycle

Steps to plan and implement security measures

Fig. 3.2.2-2 Comparison of BCPs for natural disasters and cyber attacks



Disaster BCP

Objective

How to minimize damage (disaster mitigation)
How to recover quickly (early recovery)

1) **Understanding the Business**
- Evaluate the impact on the business
- Assess the damage suffered by the core business
- Diagnose your financial situation

Factory Security Processes

Objective

Minimize damage in the event of intrusion or attack

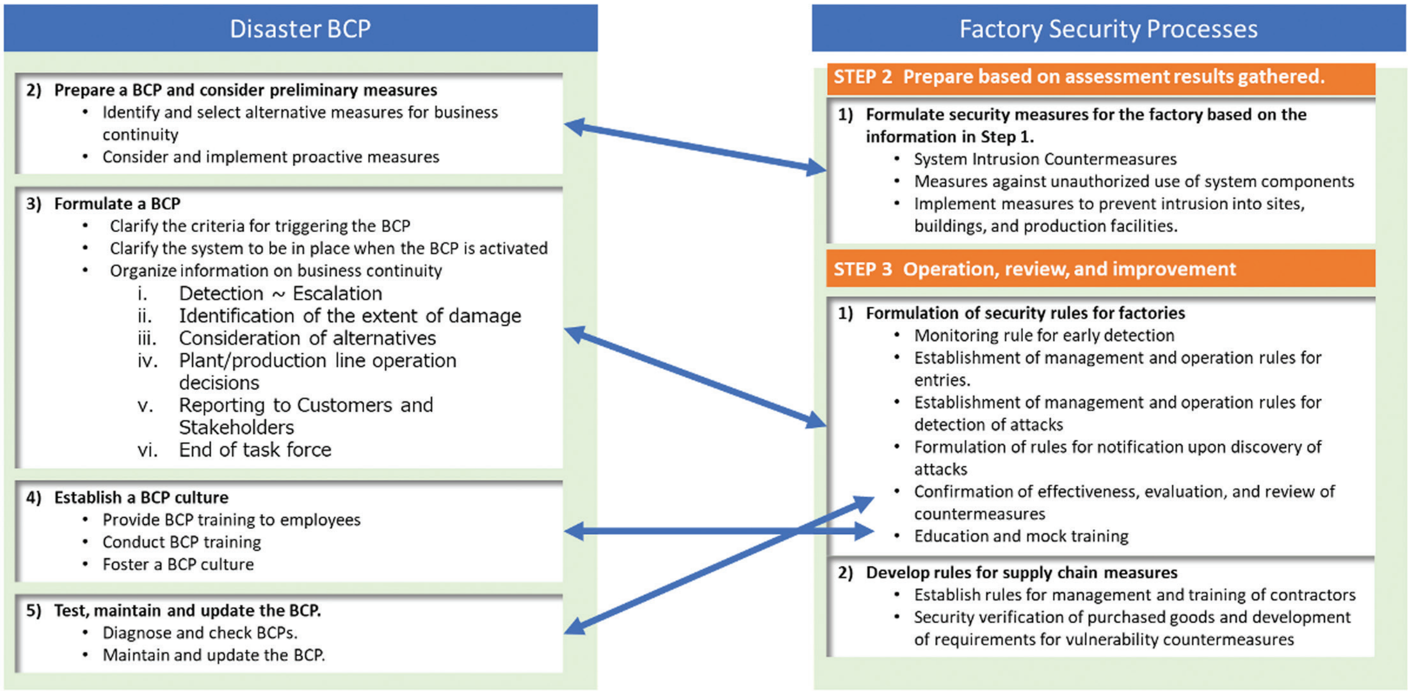
STEP 1 Gather and organize information necessary to determine preparedness (countermeasures)

1) **Factory Management Policy**
- Organize important and expanding businesses
- Organize what is needed for business continuity

2) **external cause**
- Related Laws, Standards, and Guidelines
- Stakeholders
- Requirements from the supply chain

3) **internal cause**
- Physical structure of the factory (exterior walls, building, interior structure)
- factory System Configuration
- Employee work and employment status
- Object to be protected (information, equipment, functions, etc. to be protected)
- Targets for protection.

Fig. 3.2.2-2 CONTINUED Comparison of BCPs for natural disasters and cyber attacks



Disaster BCP

2) **Prepare a BCP and consider preliminary measures**
- Identify and select alternative measures for business continuity
- Consider and implement proactive measures

3) **Formulate a BCP**
- Clarify the criteria for triggering the BCP
- Clarify the system to be in place when the BCP is activated
- Organize information on business continuity
  - i. Detection ~ Escalation
  - ii. Identification of the extent of damage
  - iii. Consideration of alternatives
  - iv. Plant/production line operation decisions
  - v. Reporting to Customers and Stakeholders
  - vi. End of task force

4) **Establish a BCP culture**
- Provide BCP training to employees
- Conduct BCP training
- Foster a BCP culture

5) **Test, maintain and update the BCP.**
- Diagnose and check BCPs.
- Maintain and update the BCP.

Factory Security Processes

STEP 2 Prepare based on assessment results gathered.

1) **Formulate security measures for the factory based on the information in Step 1.**
- System Intrusion Countermeasures
- Measures against unauthorized use of system components
- Implement measures to prevent intrusion into sites, buildings, and production facilities.

STEP 3 Operation, review, and improvement

1) **Formulation of security rules for factories**
- Monitoring rule for early detection
- Establishment of management and operation rules for entries.
- Establishment of management and operation rules for detection of attacks
- Formulation of rules for notification upon discovery of attacks
- Confirmation of effectiveness, evaluation, and review of countermeasures
- Education and mock training

2) **Develop rules for supply chain measures**
- Establish rules for management and training of contractors
- Security verification of purchased goods and development of requirements for vulnerability countermeasures

EVALUATION EXERCISE

The logic presented in this white paper is based on proven results at the author’s company and several business partners. If you have any questions about how this information can be used in the future, please feel free to contact us. Together, we can make the entire industry safer.

CONCLUSION

This white paper, the third in the series, reminds you of the risks of choosing the right consultant and misjudging the timing of consultant introduction due to the anxiety you may feel even after understanding your security policy, and introduces two ways to proceed with confidence in order to dispel any vague anxiety you may feel. I would like to introduce two ways to proceed with confidence. We are confident that you will gain confidence by using both of them.

We hope that you will gain confidence by following the recommendations outlined here, and that you will work with the consultant at the optimal time and in the optimal relationship to promote your security measures. Do not accept a pushy consultant. And I believe that as security measures are promoted at each factory, the security level of the entire supply chain will be raised and a safer digital society will be realized. Let’s work together.

In the next issue, I will explain how we should think about and proceed in a consistent manner with the many security-related regulations and standards that may seem confusing.

About the Author

As executive director of global security at NEC Corporation, a manufacturer of telecommunication equipment and components, Hiroyuki Watanabe has responsibility for cyber security, secure manufacturing, new business and sales at the company.

He has extensive knowledge and experience across various business categories. Among his notable contributions are his successes in architecture design for an exchange system, which resulted in $1B business in the 1990s. During the 2000s, Watanabe-san initiated an open source community called “Open DayLight” for IBM, BROCADE, and CISCO among others, and created and expanded the market for software defined networking (SDN).

His recent research interest includes revolutionizing legacy supply chain management, and evolution of manufacturing industry using dual-use space defense technologies.

IPC®
BUILD ELECTRONICS **BETTER**

3000 Lakeside Drive, Suite 105 N
Bannockburn, IL 60015 USA

+1 847-615-7100 **tel**
+1 847-615-7105 **fax**
www.**ipc**.org

IPC is the global association that helps OEMs, EMS, PCB manufacturers, cable and wiring harness manufacturers and electronics industry suppliers build electronics better. IPC members strengthen their bottom line and build more reliable, high quality products through proven standards, certification, education and training, thought leadership, advocacy, innovative solutions and industry intelligence.