IPC®

BUILD ELECTRONICS BETTER

KEY BUSINESS PRIORITIES TO PREVENT CYBER-ATTACKS — PART 2

Hiroyuki Watanabe: NEC Corporation
Tokyo JAPAN

ABSTRACT

In part 1 of this series, the author provided insight into how cyber attackers attempt to cripple organizations by infiltrating various systems at the “targeted” firm.

In part 2 of this series, the author provides an action plan whereby management works closely with company employees. Open communication and trust are key elements. Management and staff must work closely together to identify and prevent disruptions due to cyber attacks.

INTRODUCTION

Company management communicates to factory floor personnel only to be vigilant with respect to cyber intrusions. IT departments will often provide training related to “phishing” and email scams. However, this may not go deep enough. The factory floor workers receive this order and are confused as they do not know what to do often because requirements are vague, and they are unsure of what they must do. (1)

On the other hand, in the case where management has not yet developed a prevention program, employees may feel that security measures are insufficient. This insecurity will lead to lack of vigilance which can lead to mistakes.

Therefore, in this paper, we will cover basic concepts and direction of the assessment conducted..

IDENTIFYING THE PROBLEM

When planning cyber-attack countermeasures, costs should be aligned in a dialogue with management before specific assessments and measures are implemented. This is a major challenge. All too often, company executives make some of the following excuses when addressing cyber security:

“As a member of management, I can’t afford to spend too much. Do it without costing too much so that customers and the public won’t backlash!”

“Cyber measures are important. But we must control the spend.”

“Consumer products are cheap, so you can’t spend a lot of money on cyber security measures; just do it just right so the public doesn’t go on social media and say, ‘It’s too bad.’”

I don’t think the management of your company would make such assessments, but I also don’t think there are any executives who would say, “You have an unlimited budget, so make it perfect.

Obviously, these are not the ideal responses or attitudes.

THE ISSUE: UNDERSTANDING CYBER THREATS AND MAKING THE KEY INVESTMENTS TO MITIGATE

This is a critical issue to address. If we do not overcome this problem, we may not take this problem seriously. If this happens, you may lose business opportunities, with customers saying, "A company that can't even handle such a basic issue cannot be trusted."

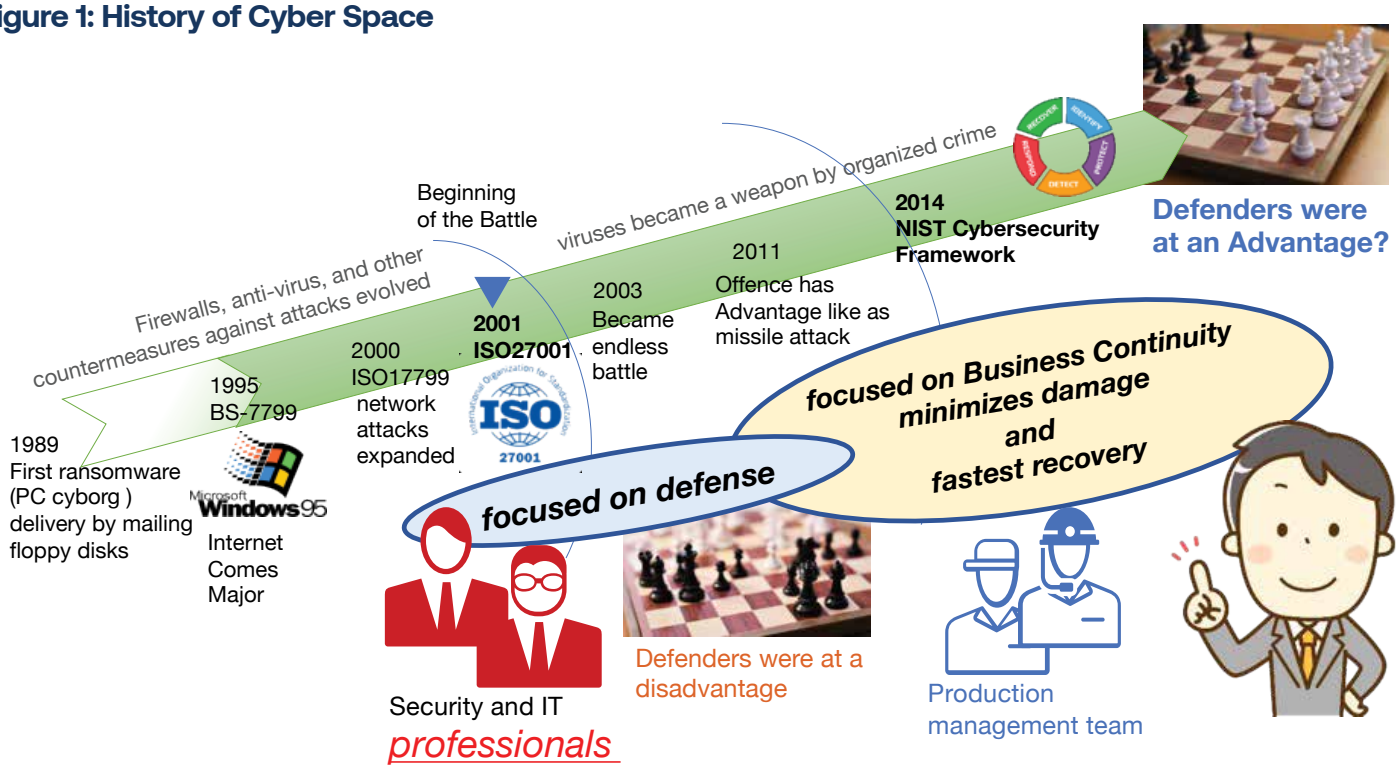
Some managers may follow their "wild guesses" and decide to entrust the work to a specialist because they do not think it can be done at their site. In this case, there is a high probability that a consultant will not understand what is required.

Therefore, the correct procedure to follow is to scale resource investment, and strike a balance between investment and business value are essential.

But can you show management your cost estimates before you start considering them? And even if you could, would you be able to explain its validity? Security measures are an endless game, not just a technical issue. The level of security measures that the public evaluated as OK yesterday may become insufficient today. It is not impossible to say that there is a ceiling because it has to be reviewed every year. Still, as a business, the only way to cover the increasing costs is to raise prices through price negotiations or reduce costs through self-help efforts.

Synchronizing an agreement with senior management that this problem can be successfully solved is a challenge. But it doesn't mean there isn't a way to solve it.

Figure 1: History of Cyber Space



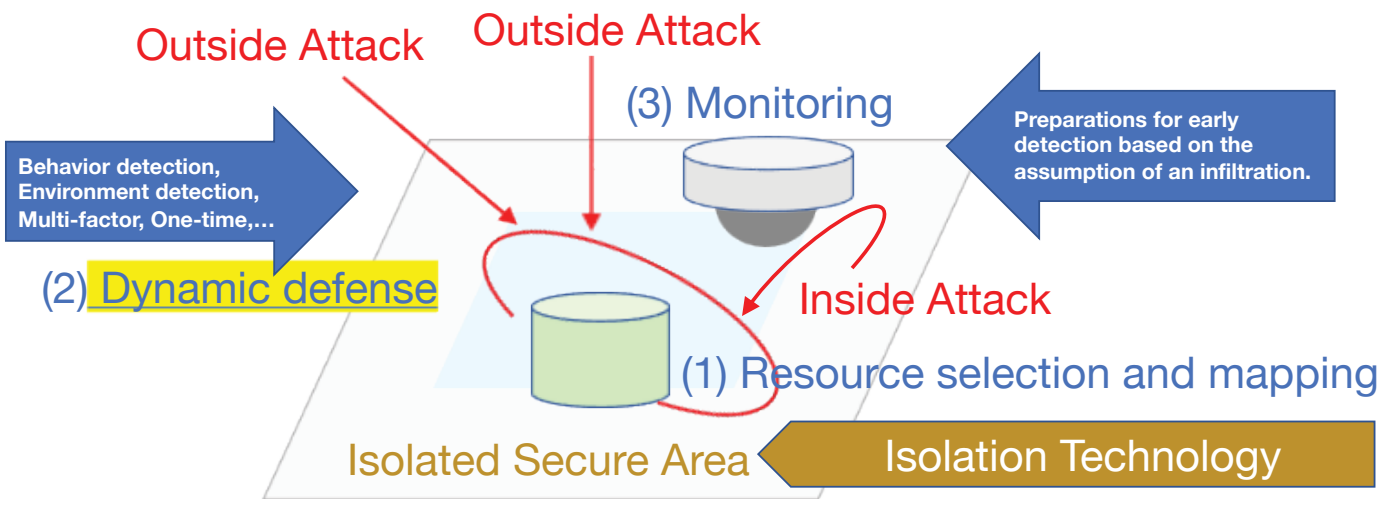
The focus has shifted from prevention through defense to business continuity (minimization of impact and quick recovery) based on the premise of intrusion, in a situation where the attacker has the upper hand. In conjunction with this change, the responsibility for countermeasures has shifted from relying solely on security and IT professionals to placing greater responsibility on the manufacturing floor, and ISO2700 and NIST's SP800 series have also been strengthened. This change in thinking toward zero-trust is the source from which "minimum safety measures" are derived.

We should first teach the zero-trust architecture to senior management. Then, next, we should explain (2) "the correct procedures to proceed," and (3) "the scale of resource input and its correctness," based on the zero-trust architecture. These will help executives understand the validity of the explanatory logic and increase their trust in the people on the factory floor. Furthermore, after creating a two-dimensional graph based on the required cost and business impact, we show how to draw a borderline to converge costs and explain (4) "balance between cost input and business value" to senior management, leading them to be able to discuss the issue together.

MAIN DISCOURSE:THE ANATOMY OF A CYBER ATTACK

Cyber attacks not only happen externally, but also from inside companies. And at some point, a situation could arise in which a break-in occurs. This is the concept of Zero Trust. In other words, the focus is on business continuity (minimization of impact and quick recovery) under the assumption that an intrusion has occurred (Figure 2). This is often known as zero-trust architecture.

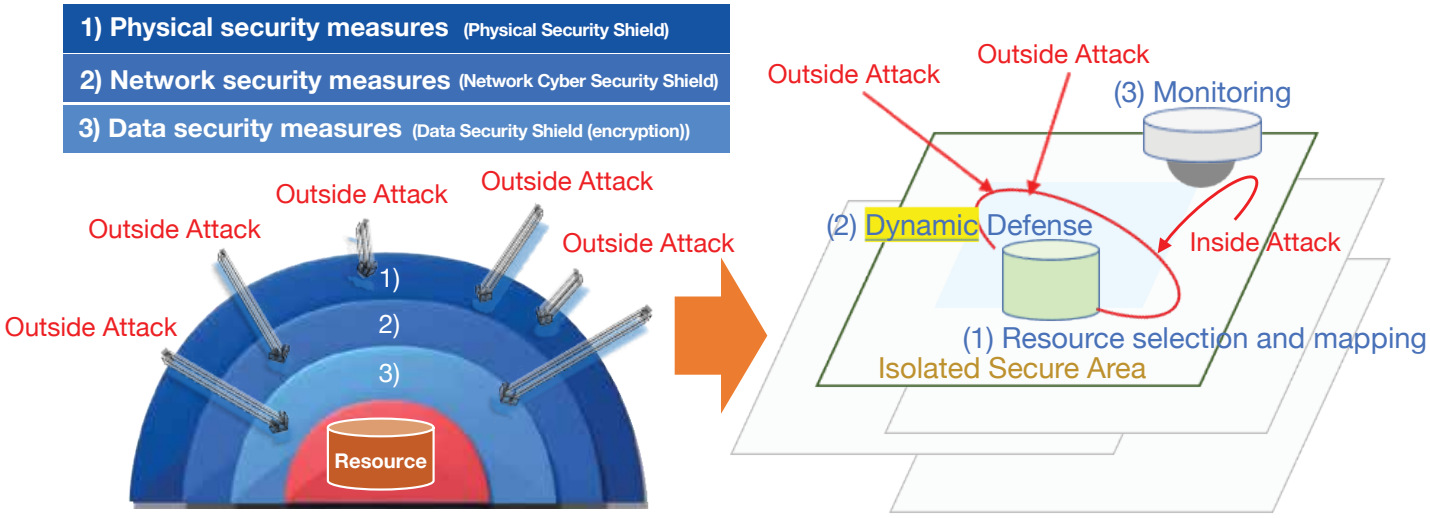
Figure 2: Basi Unit of Zero-trust Architecture



The difference from conventional countermeasures that specialize in protection from the outside is that (1) the area separation minimizes the impact range and (2) the monitoring function is provided for cases where intrusion has occurred even though the area has been protected.

[1] NIST SP800-207

Fig. 3 Before and After Zero-trust of the System.



In other words, first share with senior management that your strategy is focused on business continuity in the event of a cyber attack. Cyber attacks, like natural disasters, are regarded as "disasters that cannot be prevented" and investments should be made to prepare for them. The scale of investment will be determined by business judgment in light of the business.

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

(a) It is not visible when it occurs.

If the monitoring measures described in Figure 3 are not established and the conditions for determining that an intrusion has occurred are not determined at the outset, the initial response will be delayed. This delay will negatively impact your business. In advance preparation for monitoring the possible cyber-attack, the following two initiatives should be considered:

(i) Criteria for initiating initial response even with incomplete event detection should be determined.

(ii) Be prepared for the responsible person to immediately decide whether or not there is a business impact based on the monitoring results.

Let's review each of these points:

Initial response criteria

Since cyber attacks include unknowns, it is necessary to initiate an immediate response even if there is not necessarily a clear detection of an attack. It is necessary to determine in advance the conditions to be treated as attack detection, including access to critical resources from an abnormal route, ten or more password input errors within one minute, or two or more work instruction tablets on the manufacturing line that are slow to respond simultaneously.

Immediate decision preparation by the responsible person

It is too late to take initial action after a long period of time from the detection of a cyber-attack to the analysis of its cause and impact. For this reason, a flowchart should be prepared in advance to facilitate the process. What is the impact on the business? Has any customer data been compromised? For this reason, decisions must be made by senior executives, as responsibility cannot be fully taken at the manufacturing site.

And management needs to be made aware that if the framework for this decision is inadequate or if the speed of the decision is too slow, the company will lose the trust of customers. Since we cannot invest and prepare for costs that are not commensurate with the size of our business, management can for the first time recognize this as a critical issue.

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

In the support for disaster response, the size of the separation compartment has been considered based on the assumed impact area of a single natural disaster. For example, the manufacturing company has probably distributed parts 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. 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 that 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 should be considered in the operational rules, and the technology to realize it can be considered later.

SECURE/NOT SECURE (GOOD ENOUGH OR NOT)

Such as the term and concept of Secure/Not secure is relative, and security measures are costly and must be managed.

Even though natural disasters cannot be prevented by direct human intervention, it is possible to minimize damage and achieve early recovery. And the cost of doing so can be controlled to some extent. Zero Trust's cyber countermeasures focused on business continuity can be thought of as a detailed plan for identifying and mitigating cyber-attacks. Even if the occurrence of a cyber-attack itself cannot be prevented, by preparing a detailed plan, damage can be minimized, early recovery can be achieved, and costs can be controlled to some extent.

COST ESTIMATION AND COST REFINEMENT OF COUNTERMEASURES

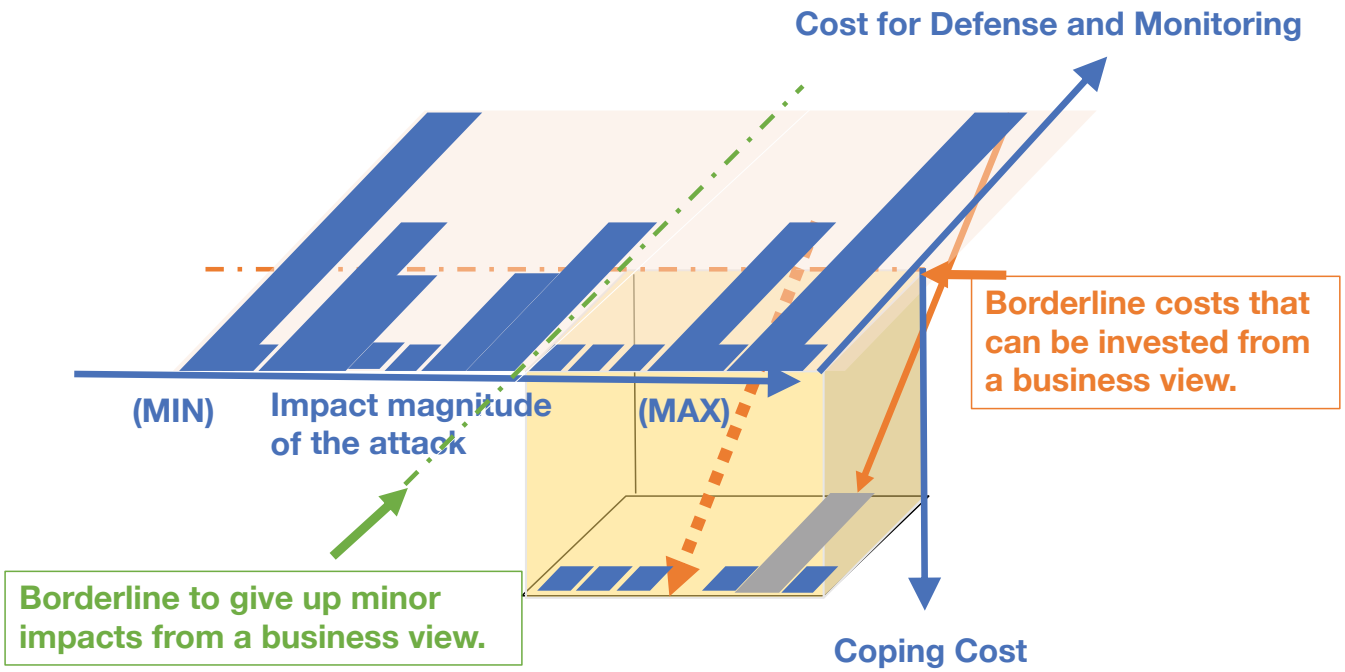
Specific countermeasures should be discussed with external IT/security service providers, using specific technologies and equipment for protection, as well as network design and operation.

In this case, the following two specifications, will be the requirements for external IT/Security service providers.

1. Definition of resources comprehensively categorized from a business continuity perspective
2. Define parcels and operations where resources are to be placed.

With this requirement, IT/security service providers will provide various proposals including cost estimates.

Figure 4: Balancing the Cost of Countermaesures



1. Resources comprehensively classified from a business continuity perspective are arranged on the X axis in order of decreasing impact. The size of the impact from a business continuity perspective depends on the definition of the compartment and operation in which the resources are placed. The definition of compartmentalized operations is also taken into account and arranged on the X-axis.
2. For each of the resources shown on the on the X-axis, the relative cost indicated by the external IT/ Security service provider on the Y-axis.
3. To get a better understanding of the cost of possible investment, one must consider the size and potential of the target business. In Figure 4, that is colored in orange.

4. In consultation with management, determine the impact borderline (the green line in Figure 4) where you will give up early detection, minimization of the impact scope, and advance preparations for early recovery. Outside of the countermeasure borderline, early detection will not be possible, and the scope of impact will be larger. However, the company will be prepared to deal with the intrusion on a one-off situation and carry out recovery activities steadily when it occurs.
5. Consider reducing the cost of the various security measures that exceed the (orange block in figure 4) cost of the resources in the green measure coverage and fit them in the yellow box in Fig. 4.
   a. Consider cost reductions carefully

      In order to keep the total cost of countermeasures for resources within the scope of countermeasures within the orange line, management should discuss with external IT/Security service providers cost reduction measures starting with items that are large outliers.

   b. Exclude some of the extracted resources

      Reexamine the definition of resources classified from a business continuity perspective and the parcels and operations where the resources are located and consider whether the operations can move them outside the borderline of the target resources with a smaller impact from a business continuity perspective.

   c. Lengthening the monitoring cycle

      The shorter the monitoring cycle, the earlier detection and detection is possible, but the amount of collected data increases, and system modification costs, such as system modification or introduction of AI for analysis of monitored and collected data, are likely to increase.

   d. Analyze monitoring information manually

      Although it is smart to store logs and use AI to analyze them, it is also wise to recognize again the value of daily visual inspections of logs by humans. As mentioned in my first paper, from a criminal's point of view, it is harder to attack a system that is well managed by humans, even if it is poorly managed, than a well-managed system that is not well managed by humans. However, it is also necessary to consider limiting the amount of log information to that which can be visually inspected.

   e. Perform human monitoring of the IT system

      Consider having the monitoring itself also conducted by a human. Even a visual check by a human on a six-month cycle is of greater value than not doing it all. If resources are not monitored and an attack occurs, one will have to go back to the first product shipped from that factory and recall it from the market. In addition, if you have manual confirmation that critical resources were in the correct state six months ago, you can be sure that products shipped earlier than six months ago are within specifications.

CONCLUSION

In this second white paper, I have provided you with material that can break down the arguments about the appropriate investment cost with upper management that you may first run into when you decide to move forward with security measures. Please utilize the “Zero Trust” basics introduced here to gain the understanding and cooperation of people on the ground, and at the same time, promote the understanding of senior management and work hand in hand with them to derive appropriate costs and countermeasure policies to promote countermeasures.

Beyond that, I believe that the security level of the entire supply chain can be raised and a safer digital society can be realized.

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.