IPC®

BUILD ELECTRONICS BETTER

UNDERSTANDING CYBER ATTACKS ON FUTURE FACTORIES — PART 1

Hiroyuki Watanabe: NEC Corporation
Tokyo JAPAN

ABSTRACT

Recently, we have seen an increase in production stoppages due to cyber attacks on just one supplier. Criminals attack the weakest link in the supply chain. However, trust in the entire supply chain, an essential countermeasure, has not been going so well. On the other hand, society is becoming increasingly digitalized, so there is an urgent need to improve the entire supply chain.

Looking inside individual companies, management is more interested in the question of how to recoup the cost of security measures than in what those measures should be. As a result, a wait-and-see attitude prevails, such as waiting until specific customer requirements are presented, or until regulations are legislated.

The only companies taking security measures are the major companies that have full responsibility for final product shipment products to their customers. And those major players challenges with their suppliers' measures.

This paper sounds the alarm that current cyber attacks upon companies pose a major business risk to the suppliers themselves, who are in a wait-and-see attitude. This paper also provides a sense of direction as to why and how to respond and that guidance does not require a large investment. This paper provides information on what needs to be done and the needed steps toward reducing business risks.

This paper will be the first in a series of four papers.

1) Understanding cyber attacks on? future factories
2) What are the priorities in the never-ending fight against criminals
3) How to choose a consultant
4) The benefits of following a non-regulatory standard

CRITICAL NATURE OF THE ISSUE

Given the reality that individual companies are making security implementation decisions based on current economic logic, the advantage of attackers who consider the entire supply chain as an attack target is likely to continue. As a result, it should be considered that the possibility of cyber attacks causing enormous damage to the entire global marketplace will increase.

Acceleration of digitalization is a necessary condition for labor force rebalancing in developed countries where the population continues to decline. If the rate of digitalization weakens, labor forces in developed countries will be competing for each other, and a situation may arise in which society cannot secure the essential workers it needs. In other words, if the speed of digitalization weakens, there is a risk that the maintenance of a strong global supply chain may not be possible.

As we will discuss in more detail later, a method in which a single company assumes overall responsibility and implements security measures independently will be more costly than one in which responsibility is shared throughout the supply chain. In addition to this, consumers must unfortunately accept the high costs of redundant supply chains. We must resolve this problem as soon as possible and come up with a system that constitutes a healthy and safe marketplace.

DIFFICULTY IN SOLVING PROBLEMS

While it would be nice if economic logic could be organized in terms of a simple interest relationship, such as who suffers the loss and who invests to prevent it, it is not that simple. Supply chains are complex, risk assessment is difficult, and the magnitude of risk changes with time and with errors. Furthermore, even the concept of countermeasures itself has changed over time. The fact that the parameters of change are too large makes it difficult to solve this problem.

A major source of confusion lies in the process of considering change parameters between quality assurance and security guarantee. Table 1shows a comparison of quality assurance and security guarantee.

Quality control aims to eliminate accidental failures, while security threat management aims to minimize the impact of malicious attacks. In quality control, the first step is to recognize cause-and-effect relationships, identify “accidental events,” control the rate and depth of acceptance testing to reduce the occurrence of problems, all while detecting root causes and applying preventive measures to halt their recurrence. Conversely, in security threat management, where “criminal malicious intent” is involved, strengthening acceptance testing does not control the occurrence of problems, nor does finding the root causes and applying preventive measures to stop them from recurring. To minimize the impact of cyber attacks, a different approach from quality assurance is essential. From this author’s experience “enhanced testing” is not a sufficient means to deal with the problem.

Table 1 Comparison of Quality assurance and Security guarantee

Item	Quality assurance	Security guarantee
Occurrence Trigger	accidental accident	malicious attack
Objective	Defect deterrence (through testing and control)	Impact minimization (Perfect deterrence is not possible)
Place of Occurrence	Can occur anywhere, but not maliciously, so can be narrowed down technically. (Why converge at x3)	The weakest point is targeted as the entry point. Attacks also evolve, so it is impossible to identify in advance where and from where they will target.)

Despite this, the culture persists that the large companies that provide end products are responsible for everything. And despite the inadequacies, acceptance testing is intensified, costs are higher, and critical industries are required to pay the costs, even if the way it is addressed is inadequate and, in some cases, inefficient.

CMMC: Cybersecurity Maturity Model Certification. CMMC is an assessment framework and assessor certification program designed to increase the trust in measures of compliance to a variety of standards published by the National Institute of Standards and Technology.

GDPR: General Data Protection Regulation.

GDPR provides for stricter protection of personal data and privacy than the EU Data Protection Directive.

In order to guarantee security, a method that can respond to any type of attack is required. Specifically, resources are classified and defined according to the impact magnitude of an attack on a specific resource. Then, appropriate protection and monitoring are prepared according to that classification in order to achieve protection and quick detection. Since the impact of a resource differs from company to company and is a trade secret of that company, the optimal solution is to share the attack risk throughout the supply chain.

The difficulty lies in the fact that it has not been possible to simply define requirements in the sense of quality assurance [where the large company providing the final product at the end of the line is made responsible for all aspects of the product]. The defense business is trying to achieve this through a combination of many regulations. However, this has not yet reached perfection, including CMMC . On the other hand, methods such as GDPR that make all companies obligated to report within a certain timeframe, are becoming more widespread.

PROPOSED APPROACH FOR THIS PAPER

The main approach of this paper is to take a broad view of the changes in each area of security and get a sense of the direction of security measures. After that, I present my thoughts on [what should be done] based on the direction. By taking this approach, I hope to help the reader understand the cause-and-effect relationship between the perception of the issue and what needs to be done.

In addition , I show the barriers to action that are faced after understanding what needs to be done on the table, and also present information that will help the reader move forward with security measures.

MAIN DISCOURSE

When one considers the various security concerns described in Section 2, many issues and roadblocks remain:

- Endless battles with criminals, i.e., endless investments
- Difficulty in recovering costs for security measures
- Lack of IT engineers
- Increase in nation-backed attacks
- Conflict between the U.S. and China

Therefore, in this paper, I address changes based on the time axis of 20 years ago, now, and 20 years from now, and organize what we should accomplish. We would like to think about this so that we can realize what we need to accomplish and draw a roadmap with a sense of background awareness and goals.

DIFFERENCES FROM 20 YEARS AGO AND EXPECTATIONS FOR THE NEXT 20 YEARS

Since the world's first ransomware (PC cyborg) delivery in 1989 was by mailing floppy disks, I think it is safe to assume that network attacks expanded in 2000. At the same time, firewalls, anti-virus, and other countermeasures against attacks evolved. 2001 was also the year when ISMS (ISO27001) was first created. However, that was just the beginning of the battle. Around 2003, viruses became a weapon used in organized crime, and there was a major shift to monetary purposes, and the fierce competition between attacks and defenses became an endless battle. And it was at the beginning of this battle where defenders were at a disadvantage, evidenced by the fact that the cost of instantly detecting and intercepting a missile is much higher than the cost of launching it.

A recognition of this fact led to the publication of the NIST CSF in 2014. To put it simply, the thinking switched from the initial ISMS, which focused on defense, to the NIST-CSF, which assumes that break-ins will occur and minimizes damage. It was suggested that encryption can be broken, walls can be breached at some point, and that priority should be given to detection through multi-faceted segmented protection and paired monitoring, rather than to network intrusion prevention on one aspect of the entire site.

And the reality is that very few people in our electronics manufacturing industry are aware that this change has shifted the players in security measures from IT engineers to the manufacturing floor.

Why have cyber attacks evolved in this way in 20 years? Just as defenders have shifted their focus from simple defense to detection, it is a natural progression for attackers to shift their focus from "the ability to break through defenses" to "stealthiness to avoid detection." This author believes that it is possible to nullify detection by preparing a multifaceted defense and not only monitoring in pairs within a site, but also by expanding the scope of monitoring and understanding inconsistencies over a wide area. A multifaceted detection network can be a turning point in an attacker's disadvantage because it increases the cost of countermeasures for criminals to break through the detection network. However, multifaceted detection networks require international cooperation, which is not easy to achieve.

Table 2 (below) reviews the findings. At this point, it still appears to be in our best interest to wait for customer requirements from a cost recovery perspective.

However, intrusions due to attacks will occur at some point. When it does occur, what will happen? In the current public opinion, large companies will likely be held responsible. However, will large companies continue to order from suppliers that caused the problem? Suppliers may be able to excuse the intrusion itself. In retrospect, the supplier will not be able to excuse inadequate protection or a significant delay in detection.

The AIDS Trojan, also known as the PC Cyborg virus, was the first ever ransomware virus documented. It was released via floppy disk before most of us ever had the opportunity to touch a computer in 1989.

The British Standards Institution's BS-7799 in 1995 was the beginning of ISMS. It was internationalized and published as ISO17799 in 2000, and later evolved into ISO27001.

The NIST Cybersecurity Framework is a set of guidelines published by the National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and practices to mitigate cybersecurity risks for organizations, version 1.0 was released in February 2014. It adds a new option to the framework for reviewing and promoting security measures, which had previously been the sole domain of ISMS.

The term [zero trust] was applied to this concept around 2020, but the concept has not changed since 2014.

When the difference between quality and security is better understood, public opinion will change from putting responsibility on a single large company to responsibility on the whole supply chain.

In other words, you must be prepared to quickly become detectable, and you must be willing to characterize your own level of defense as acceptable to public opinion. You cannot wait for the customer's request. If you make a mistake in this response, you could run the risk of losing business.

Table 2 below draws a comparison on how companies and governments are managing and responding to cyber security risks:

Table 2

	20 years ago	Today	The next 20 years
Added Architecture	Build a defense network with external intrusion barriers at the network perimeter + anti-virus software to disable attacks	Classify and define resources by impact size, map them to multifaceted security domains, and provide a set of defenses and monitoring for those resources.	Multidimensional anomaly estimation using a learning engine (Invariant Analyzer) by defining invariant relationships in the supply chain
Attack point	Intrusion from Public network into the target company	Multifaceted with the target company's network external, internal, and supply chain	
Sense point	External entry point for the subject company.	Target company network, personnel, supply chain and multifaceted resource access points	Inferential integrated detection formed by a consortium of companies
Responsibility for damage suffered	Large companies supplying the most downstream products		Share responsibility within the corporate coalition within supply chain.
Main player in countermeasure design	IT Engineer + Network Design	OT Engineer + Management	DataExchange Coordinator + Learning Engine
Cost Evaluation	Offensive cost < Defensive cost	Offensive cost < Defensive cost Defense with coping strategies (cost reduction) Enhanced detection, shorter response and recovery times = minimized impact	Cost of offense = Defensive cost Attack cost < Defense cost Detection avoidance cost > wide area detection cost (consistency basis)
Scope and scale of damage from cyber attacks	Limited area, focus on National defense National defense > Infrastructure >> General society	Increased digitalization of infrastructure expands scope of impact to critical infrastructure National defense > Infrastructure > General society	Further digitalization will expand the social impact of mass-produced equipment to the same level as infrastructure projects National defense > Infrastructure = General society
Cost recovery	Large magnitude impacted customer payments (ex. National defense)	Large magnitude impacted customer payments (ex. Defense, Critical infrastructure)	Society as a whole
Standard	Initial ISO27001(ISMS)	NIST CSF or ISO27001 (including options.)	Could by Private international standard

In part 2 of this paper, I will provide additional strategies to detect and prevent cyber attacks and protect your company's valuable AND confidential data.

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.