

Method for Achieving Cyber-resilience against Threats to Future Society

#Disaster Prevention and Resilience #Security #Digital Solutions

Author

Kazuya Yonemitsu

Managed Security Services Department, Security Cyber Resilience Division, Security Solutions Business Division, Hitachi Solutions, Ltd.
Current work and research: Security consulting, incident handling, and related activities

Kenichi Inomata

Managed Security Services Department, Security Cyber Resilience Division, Security Solutions Business Division, Hitachi Solutions, Ltd.
Current work and research: Managed security services, security information and event management (SIEM), security diagnosis, and related activities

Hideki Shimizu

Security Consulting Department, Security Cyber Resilience Division, Security Solutions Business Division, Hitachi Solutions, Ltd.
Current work and research: Security consulting

Highlight

Cyber-resilience has attracted attention over recent years as the threat of cyberattacks has grown internationally. Cyber-resilience is the ability of an information system to anticipate, withstand, rapidly recover from, and adapt to any cyberattacks mounted against it, thereby maintaining the continuity of important business operations.

Hitachi Solutions, Ltd. has developed a method for assessing the cyber-resilience of its corporate clients that can help them improve their capabilities.

This article provides a summary of the development process, the method itself, and the know-how acquired through a demonstration project.

1. Introduction

As the threat of cyberattacks grows internationally, companies are now well aware of the damage that such attacks can cause and the serious business risk they pose. Many companies have already taken action against potential damage by improving their security incident response capabilities, including by acquiring International Organization for Standardization/International Electrotechnical Commission 27001 (ISO/IEC 27001) certification and by establishing a computer security incident response team (CSIRT). This environment has seen more attention being paid to cyber-resilience over recent years. Cyber-resilience is the ability of an information system to anticipate, withstand, rapidly recover from, and adapt to cyberattacks. By improving this capability, companies can maintain information system availability and enhance the continuity of important business operations.

2. SP 800-160 Vol. 2 Rev. 1

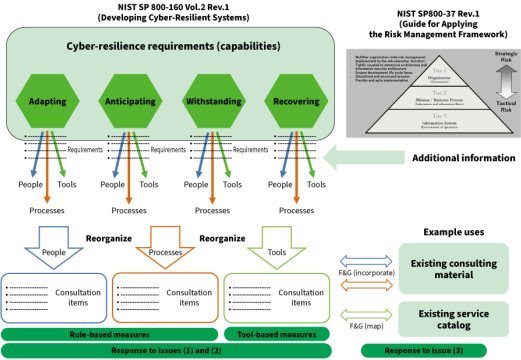
What led to the term “cyber-resilience” gaining international currency was a document entitled: SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach⁽¹⁾ (SP800-160v2r1). As indicated by its title, SP800-160v2r1 collates the engineering considerations for developing cyber-resilient systems. It defines the four capabilities of “anticipating,” “withstanding,” “recovering,” and “adapting” to adverse conditions as one aspect of cyber-resilience and provides guidance on how systems can improve these. It also explains the framework and collates the specific requirements for systems.

3. Issues with Corporate Use of SP800-160v2r1

SP800-160v2r1 is a useful reference when assessing the cyber-resilience of an information system. Using it to assess the cyber-resilience of a company, however, poses a number of problems. For example, given that companies have a large number of different types of information systems that interoperate with one another, attempting to apply requirements for individual systems as specified in SP800-160v2r1 raises the following issues, (1) it is difficult to determine which information systems at a company to include in the assessment, and (2) the person doing the work needs to determine for themselves how to assess the many different security requirements specified in SP800-160v2r1. Moreover, even if these issues are overcome, another issue is that, (3) the specific method of bridging the gap between the requirements and the current situation depends on the knowledge and experience of the person doing the work.

In response, Hitachi Solutions, Ltd. has reviewed the content of SP800-160v2r1 and developed its own evaluation criteria to overcome the above issues. In practice, this involves using the business impact analysis (BIA) methodology that Hitachi Solutions uses in its consulting service for business continuity planning. This addresses issue (1) by determining which systems to include in the assessment. Next, Hitachi Solutions reorganized the many requirements specified in SP800-160v2r1. Typically, a number of different methods are available for fulfilling security requirements. These can be divided into two categories. Rule-based measures are those that collate these methods and implement them through manual operation and rule-making. Tool-based measures, meanwhile, are those that are implemented using application software functions and software operation. Hitachi believes that issue (2) can then be resolved by enabling an objective review of the company’s existing cyber-resilience capabilities that covers the rules and security software they have in place. To deal with those cases where rule-based and tool-based measures on their own are insufficient, issue (3) can be resolved by linking together the extensive range of existing solution options available from Hitachi Solutions and presenting these as a solution map. Figure 1 shows the sequence of steps whereby Hitachi Solutions developed its own evaluation criteria from SP800-160v2r1.

Figure 1—Sequence of Steps Hitachi Used to Develop its own Evaluation Criteria from SP800-160v2r1



F&G: fit and gap, NIST: National Institute of Standards and Technology
Hitachi developed its own evaluation criteria for cyber-resilience to resolve the issues posed by SP800-160v2r1.

4. Study and Feedback on Proposed Solution

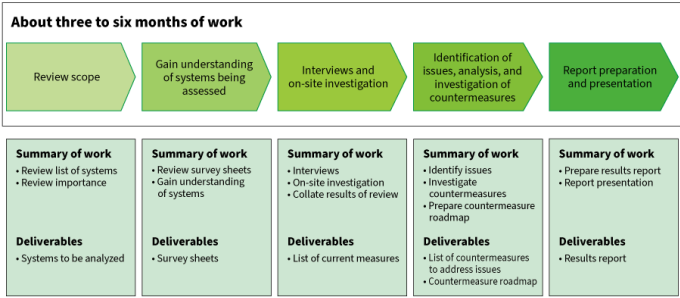
Having decided how to go about resolving each of the issues, Hitachi Solutions began working on these solutions with a view to ultimately establishing them as an assessment service that could be incorporated into its menu of consulting services. Details of this study are described below.

4.1 Development of Assessment Service

The assessment service produces a report for the client after having first conducted consultant interviews to review their cyber-resilience and identify where it can be strengthened. Figure 2 shows the assessment process.

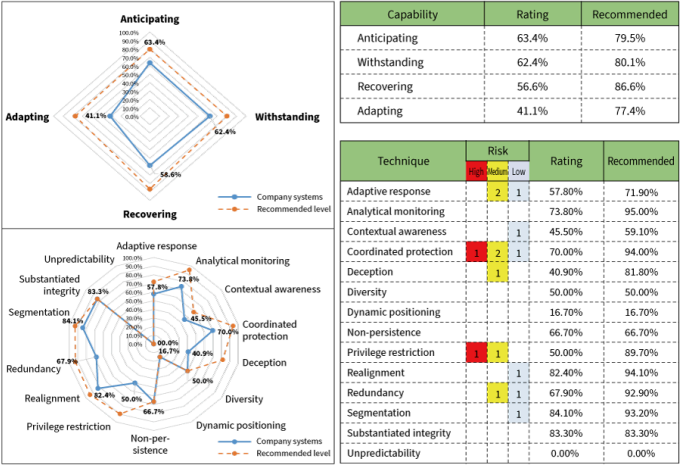
The BIA method with which Hitachi Solutions is already familiar is used to review the scope. This step involves identifying the systems that the company employs in its important business and operational activities to determine which ones are to be assessed. In the “gaining an understanding of the systems” step, documents provided by the client are used to determine the system environment, including the network configuration, what the systems are used for, and by whom, and also to obtain an overview of system operation and security measures. This understanding informs subsequent steps so that they can be performed accurately. The “interviews and on-site investigation” step involves talking to the customer with the aid of a checklist to determine and assess current cyber-resilience. This checklist was put together by Hitachi Solutions in such a way that assessment can be made on the basis of the four capabilities and 14 techniques that break these capabilities down into resiliency methods, as specified in SP800-160v2r1. The “identification of issues, analysis, and investigation of countermeasures” and the “report preparation and presentation” steps use the information obtained during the previous steps in the process as input and put analytical methods in place that can deliver visual output that is easy to understand. This is done in a way that makes it easy for the client to see for themselves where problems exist (see Figure 3).

Figure 2—Assessment Process



The service establishes an assessment process for reviewing a company's cyber-resilience that clearly specifies the work to be done at each step and the associated deliverables.

Figure 3—Easily Understood Visual Output



The report lists the actual and recommended ratings for four capabilities and 14 techniques to provide an easily understood visual representation of current risks.

4.2 Demonstration Project and Feedback

To determine whether the new assessment service really could perform the meaningful evaluation it was intended to provide, a demonstration project was undertaken that encompassed six systems across three companies. The results indicated a number of problems where improvements were needed. One problem was that the amount of time needed for the consultants to carry out the demonstration project interviews greatly exceeded expectations. This arose from a mismatch in understanding cyber-resilience between the consultants and the people being interviewed. More interview time than expected was taken up in explaining the reasons why particular questions were included.

There is a considerable degree of overlap between the requirements specified in SP800-160v2r1 and those that traditionally apply to information security. While there are certain requirements that arise out of cyber-resilience specifically, the number is comparatively small. That is, while cyber-resilience can be seen as providing a new way of looking at security measures, knowledge of existing information security provides the basis for understanding this approach.

When making settings changes to ensure that a proxy server blocks unauthorized communications by a confirmed malware infection, for example, conventional information security requires a standardized procedure for specifying how to do so. Cyber-resilience, on the other hand, has the additional requirement that settings changes be made without shutting down the information system. It is the part about not shutting down the system that is crucial. Depending on how much the interview subjects knew about information security, it took an unexpected amount of additional time for them to appreciate this point.

This problem was addressed by modifying the interview questions. To promote understanding of cyber-resilience by interview subjects and to minimize the time taken to obtain responses, the questions were changed to explicitly ask about use of the rule-based and tool-based measures that the consultant wanted to find out about for the assessment. In the case of the above example, subjects were questioned about specific situations, asking whether operational rules are in place for changing settings “without shutting down the information system” when such and such a situation occurs, emphasizing those phrases that relate to aspects of cyber-resilience. By doing so, the time taken to conduct interviews was brought back within initial expectations. While there were concerns that this would lead interview subjects to respond on the basis of a lack of understanding of what cyber-resilience really is, in practice there was no loss of assessment accuracy and most cases of an interviewee having difficulty answering were dealt with by talking through the basis of what the question was about.

4.3 Creation of Solution Map

The assessment service includes a report presentation to highlight where improvement is needed. This presentation must be such that the client is left with a clear idea of the actions they need to take. To this end, a solution map was created to show which of the available solutions from Hitachi Solutions are relevant to each of the improvement points likely to be suggested in the presentation. Hitachi Solutions offers total security solutions and has an extensive menu of solution options. Hitachi offers both consulting service solutions for implementing rule-based measures and package system integration (SI) service solutions for implementing tool-based measures. The map shows that most of the improvement points can be dealt with by these options. To deal with the remaining improvement points for which no such solutions are available, Hitachi Solutions augments its existing solutions in ways that include incorporating promising products identified from product information held by overseas offices or obtained from overseas security conferences that it has attended in the past. In this way, it is able to offer solutions for all of the improvement points.

5. Conclusions

Given that there is something of an arms race going on between cybersecurity measures and attackers, it is important to review and improve security measures. Strategies for preventing such outcomes feature heavily in security measure trends and developments. It is anticipated that cyber-resilience will be a lead strategy in this area over the coming years. By improving the cyber-resilience of its corporate clients, Hitachi Solutions intends to play its part in maintaining safety and security in future societies as exemplified by Society 5.0.

REFERENCES
1) The National Institute of Standards and Technology, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST SP 800-160 Vol. 2 Rev. 1 (Dec. 2021)

Hitachi Review

Hitachi Review is a technical medium that reports on Hitachi's use of innovation to address the challenges facing society.

The *Hitachi Review* website contains technical papers written by Hitachi engineers and researchers, special articles such as discussions or interviews, and back numbers.

Hitachi Hyoron
(Japanese) website

<https://www.hitachihyoron.com/jp/>



Hitachi Review
(English) website

<https://www.hitachihyoron.com/rev/>



Hitachi Review Newsletter

Hitachi Review newsletter delivers the latest information about Hitachi Review when new articles are released.