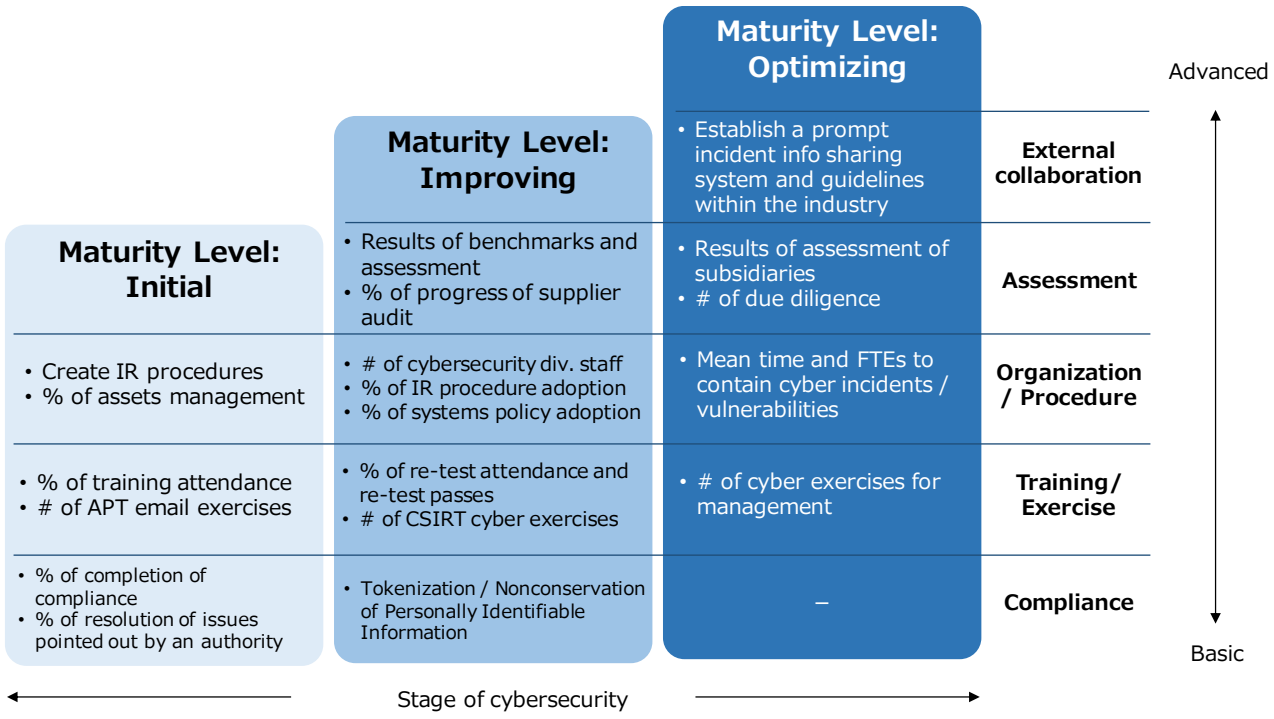
April 2019

Cybersecurity KPI Model

【Outline】

- As business depends more and more on digital technology, the impact of cyber risks increases. The greater the threats posed by the cyber world, the greater the difficulty for a single organization to reduce the number of cyberattacks. However, potential financial impacts from cyberattacks can be reduced through the efforts of management and staff.
- To reduce the potential financial impact and to promote digital innovation, JCIC has developed an original model, *the Cybersecurity KPI Model* (see Figure 1), through interviews and surveys. On the basis of this model, cybersecurity managers should identify their KPIs in accordance with the maturity level of their organization in regards to cybersecurity at the beginning of the fiscal year. This model will be updated on the basis of feedback from companies of many different sizes and from multiple industries.
- Organizations ought to identify the purpose of cybersecurity for their organization before setting up their KPIs. Management and cybersecurity managers should discuss what their organization's vision and strategy are, and what risks it would face. These discussions will contribute to identifying their KPIs.

(Figure 1) Cybersecurity KPI Model



1. Cybersecurity KPI Model

■ Overview

JCIC has developed the Cybersecurity KPI Model by gathering 47 KPIs from interviews and other research and allocating them into three maturity levels.

The horizontal line in this model shows the cybersecurity maturity level, and the vertical line shows the category of activities with regard to cybersecurity such as external collaboration, assessment, organization/process, training/exercises, and compliance.

■ How to utilize the Cybersecurity KPI Model

On the basis of this model, cybersecurity managers can identify KPIs according to their maturity level at the beginning of the fiscal year. It is not necessary to follow this model strictly, but cybersecurity managers can customize these KPIs in accordance with their organization's status.

(Figure 2) How to utilize the Cybersecurity KPI Model

Item	Description
Target Audience	CISO (Chief Information Security Officer) and manager of cybersecurity division
When to utilize	At the beginning of the fiscal year
How to identify KPIs	First, select your organization's cybersecurity maturity level on the horizontal line. Next, identify your focus activities (KPIs) from the vertical line and obtain approval from your management. Lastly, set up a detailed plan to achieve KPIs and distribute them to your staff.
Benefits of KPI model	• Ability to identify an organization's KPIs according to maturity level • A ability to evaluate performance objectively • Reduction of the potential financial impact

■ Further steps

This model will be updated on the basis of feedback from companies of many different sizes and of multiple industries. In addition, it seems to be necessary for JCIC to try to implement further research, such as on the relationship between the Digital Transformation (DX) of an organization and its KPIs, on how to collect KPI related indicators automatically, on how to deal with cybersecurity KPIs for their products, on how to measure the attitudes toward security of an organization by using KPIs, and the like.

In our interviews, we found that some organizations use "KRIs (Key Risk Indicators)" to visualize their cyber risks rather than KPIs. JCIC will introduce KRIs in the next report.

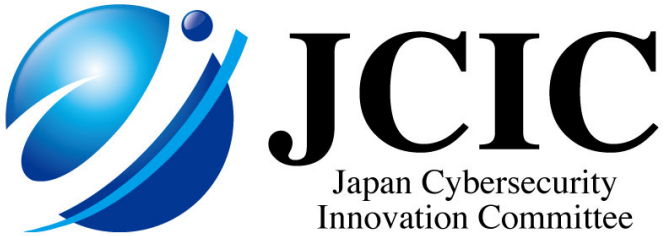
2. Conclusion

This report illustrates JCIC's original model, *the Cybersecurity KPI Model*, to reduce the potential financial impact and to visualize cybersecurity. Using this model, cybersecurity managers can identify their KPIs at the beginning of the fiscal year in accordance with their maturity level.

If it is difficult to choose which KPIs should be set up, JCIC recommends that management and cybersecurity managers return to basics, such as asking, "What is the purpose of cybersecurity at your company?". They should discuss what their organization's vision and strategy are, and what risks it will face. These discussions will contribute to identify their KPIs.

Discussing cybersecurity goals with management, cybersecurity managers and related divisions, and reporting performance to management on a regular basis, a cybersecurity culture can be built within the organization. Such culture contributes to increasing budgetary and human resources for cybersecurity.

To establish a secure and safe digital society, cybersecurity visualizing activities should be leveraged by not only single organizations or industries, but by all facets of business and society.



[Author]

Kenji Uesugi, JCIC Senior Fellow uesugi@j-cic.com

Toshihiro Hirayama, JCIC Senior Fellow hirayama@j-cic.com