April 28, 2022
Carbon Solution Business Unit
IHI Corporation

Cyber Security Incident Response Policy During the Holidays (Notification)

Dear All,

The risk of cyber attacks has been increasing recently, and various companies and organizations have been victims of ransomware and other cyber attacks. Therefore, assuming that PCs and Servers of the IHI Group are compromised during the holidays, IHI will strengthen Cyber Security Incident Response Policy. We kindly request you to take the following actions.

1. Criteria for Cyber Attacks

Among the four types of security alerts (Informational, Medium, Serious, Critical) that determined by the Global SOC, Critical and Serious alerts are identified as cyber attacks.

2. Response Policy for Cyber Attacks

(1) When a compromise for PCs or Servers is detected in an organization that has installed security monitoring tools, the Global SOC immediately will isolate the compromised devices from the network through remote operation.

(2) The Global SOC will inform the Security Person of Contact and the Information Security Department of IHI by e-mail.

(3) Information security department of IHI will notify the following members by e-mail that the compromised devices have been isolated and the status of the compromise.

To: Information Security General Manager (President) of the subsidiary in charge of the compromised devices, Information Security Subcommittee member, Security Person of Contact

CC: Chairman of the Board, President, Executive Vice President, General Manager of Intelligent Information Management Headquarters of IHI

(4) Information Security Department of IHI will hold a countermeasure meeting. The attendees are Information Security General Manager of the subsidiary in charge of the compromised devices, Information Security Subcommittee member, Information Security Manager and Security Person of Contact. At the countermeasure meeting, the following items will be discussed and implemented according to the action item lists and their assignment table as decided by this meeting.

・Necessity of reporting to stakeholders, including relevant ministries and agencies
・Measures to prevent the spread of damage
・Methods to continue operations without the system
・System recovery methods
・Incident response framework (action item lists and their assignment table)

3. Revision Reason of Response Policy for Cyber Attacks

The Global SOC monitors the network 24 hours a day, 365 days a year, and when critical or serious alerts are detected from PCs, the PCs are forcibly isolated. However, the Servers are manually isolated after sending an e-mail to the Security Person of Contact because of the impact on business operations. Therefore, the network isolation of the Server is not immediately implemented, which may lead to the expansion of the compromise to other Servers. IHI will revise the response policy to implement network isolation even for Servers when the Global SOC judges that the alert is critical or serious.

4. Request

Please inform all employees of the Cyber Security Incident Response Policy.

5. Effective Date of this Response Policy

April 28th, 2022

Sincerely yours,
K.Sakamoto