Cybersecurity Implementation and Consultation /
Cyber Threat Monitoring Services

Kajima Corporation

KAJIMA CORPORATION

Standardizing cyber threat responses for all overseas subsidiaries
Building a globally trusted IT environment

Hajime Kawamura
General Manager
IT Solutions Department
Kajima Corporation

Satoru Otsuka
Senior Manager
Information Infrastructure Group
IT Solutions Department
Kajima Corporation

Lala Doma
IT Manager
IT Department
Kajima Overseas Asia (Singapore) Pte. Ltd.

Liew Chiat Ming
Assistant IT Manager
IT Department
Kajima Asia Pacific Holdings Pte. Ltd.

Customer profile
Kajima Corporation
Address: 1-3-1 Moto-Akasaka, Minato Ward, Tokyo
Founded: 1840
Capital: 81.4 billion yen
Net sales: 2,391.5 billion yen (FYE March 2023)
Employes: 8,129 (End of March 2023)
Business: Civil engineering, equipment installation, and a wide variety of other businesses related with a focus on contracting and outsourcing and other general construction. Under the vision statement of "Willingness to take on new challenges leveraging the power of ideas and technology to make imagination and amazement a reality" As a group of individuals working together as one, the company pursues creative progress and development founded on both rational, scientific principles and a humanitarian outlook, through which the company strives to continually advance business operations and contribute to society.
URL: https://www.kajima.co.jp/

Overview

Challenges
New and increasingly frequent security threats necessitate Kajima Group to standardise and strengthen its IT security measures.

There were differences in the status of IT security measures at each overseas subsidiary.

The company wanted to promote standardization and strengthen controls but had difficulty securing security personnel internally.

Results
Visualized the security measures desired by Kajima Group.
Used NEC's deep expertise and knowhow to define the security standards required for the entire group.

Achieved visualization and standardization of the security measures status of each overseas subsidiary.
Engaged in close-knit communication with each subsidiary to raise the overall security level by adopting security solutions and drafting operating guidelines.

Built a sustainable IT environment.
Established a socially healthy and reliable IT environment that is trusted by customers and employees in all global regions.

Solutions

NEC Asia Pacific's Advanced Response Centre (ARC)

SOC monitoring / Operations & Defense

24/7 monitoring service by NEC Asia Pacific's Advanced Response Centre (ARC)
The NEC team of security specialists provides support, from consulting to secure system integration and management. It supports integration and permeation at each overseas subsidiary, including the 24/7 monitoring services above.

Challenges

How to build a trusted IT environment for the entire Kajima Group's global footprint

Since its founding in 1840, Kajima Corporation has aimed to create a society in which people can live in peace and comfort. The company has contributed to the advancement of industry and society through its construction activities. With an "enterprising spirit" through which the company aggressively and boldly pursues new challenges, Kajima Corporation identifies changes in society and embraces the challenge of creating truly pleasant environments to provide high value-added services on a global scale. In the Southeast Asia region, in addition to its construction and development business, the company established an open innovation hub to accelerate digitization of its business in the built environment sector.

To stay ahead of the curve in an everchanging world, the company is promoting digital transformation (DX) in business to aggressively apply the power of technology towards transforming existing workflows and the organizations engaged in those operations. However, while corporate digitalization made it cheaper and easier to share and utilize information of value, this also led to an increase in risks such as theft, leaks, and manipulation. To address these risks, the company also engaged in efforts to strengthen its digital security. "I feel the importance of security every time I see news related to ransomware attacks or data breaches due to unauthorized access. Information management has become increasingly important," said Hajime Kawamura of Kajima Corporation.

Kajima Corporation conducts business in countries around the world, with business operations and the scope of business varying depending on the country and local subsidiary. Also, workflow digitalization was being implemented by having each local subsidiary based on their individual status. "There were differences in the IT (digital) security measures of each company, so we have been thinking it was necessary to achieve a consistent level of security for the entire group," said Satoru Otsuka of Kajima Corporation.

Why NEC?

NEC's vast knowhow related to overseas security governance

To ensure improvements to overall security measures by local subsidiaries, Kajima Corporation chose NEC as their partner for external expertise. Reflecting on the start of the project, Otsuka noted, "We knew that NEC had vast experience and a solid track record for monitoring services to address cyberattacks, so we wanted to ask for their support in strengthening security at our overseas businesses."

Using NEC's deep expertise and knowhow, the project began with visualizing the current status of security measures and outlining an overall concept of the security measures desired by Kajima Corporation. To create a solid image of security measures, Kajima involved representatives from 14 local subsidiaries in eight countries in Asia to decide on a project team, service level, and implementation schedule.

However, Kajima Corporation's overseas business is a conglomerate of operating companies engaged in various business sectors and comprised of various operating structures. There was also no existing framework for how to manage the security measures of each company based on the same consistent standard. Kajima and NEC worked together to establish clear channels for smooth communication. "NEC provided flexible support based on the status of each company, including providing online preliminary meetings and integration support," noted Liew Chiat Ming of Kajima Asia Pacific Holdings Pte. Ltd., who oversaw local integration at 14 local subsidiaries and sites.

Kajima was concerned about the risk of data leaks and unauthorized access associated with consigning security measures to an external partner. To navigate potential hurdles, Kajima and NEC collaborated to clearly define deliverables and performance evaluation methods. "Creating contracts that addressed those risks by outlining stringent security measures and compliance rules enabled us to mitigate risks," he noted.

Lala Doma of Kajima Overseas Asia (Singapore) Pte. Ltd., who oversaw integration at four subsidiaries in Singapore, noted, "Practical metrics based on the status of each company, milestones and a reporting mechanism were defined, so we were able to complete the project, including integration, within the goal timeframe. NEC's support has also helped us save time and resources that would have otherwise been spent on the project. I am also very satisfied with the fact that this project enables us to provide a more secure work environment for our employees."

As head of company-wide governance, Otsuka oversaw the project from the Tokyo head office. "Even after implementation, the NEC team continues to follow up with us to ensure peace of mind in system operations," he noted.

Results

Enhanced overseas security governance and contributed to the formation of a sustainable IT environment

One of NEC's implemented security measures is centralized monitoring services 24 hours a day, 365 days a year. This enables the visualization of security threats and the status of measures, which previously were being addressed on a company-specific basis, via a single report.

Otsuka praised the project, saying, "Enabling status confirmation even from Japan has increased the level of our security response and enhanced our security governance. Overseas business faces various problems that differ depending on the local company, so this project made me realize NEC's ability to work with customers on evaluating and resolving each problem."

Looking back on the project, Kawamura added, "Companies like NEC, which can provide Japanese security specialists to take a central role not only in system architecture but also in follow-up support, are rare. I felt that they were an invaluable part of our creating a security governance structure."

The duty of the IT Department is to build a sustainable IT environment, stated Kawamura. "To ensure that we remain a company that is trusted by the customers and employees who use our IT environment as well as a company that is healthy and trusted by society, it is critical that we strengthen our global information security. I think this project demonstrates a solid method of resolution even amid difficulty in securing security personnel."

Focusing on the stable operations of the constructed framework, Kawamura noted, "I hope that we will be able to collaborate with NEC to address the new security threats that arise with advancements in IT."