IMPROVE RESILIENCE IN THE FACE OF CYBER THREATS

Honeywell's portfolio of cybersecurity software and services helps one of the world's leading financial institutions protect their Operational Technology (OT) environment and enhance their cybersecurity posture.

Case Study

Honeywell

OVERVIEW

To help promote optimal protection and system connectivity, one of the world's leading financial institutions turned to Honeywell to enhance its cybersecurity. The project scope covered multiple buildings that would accommodate thousands of employees. Project officials chose Honeywell as they wanted a trusted advisor with experience in identifying and procuring reliable cybersecurity software and services, along with best practices, careful planning, and step-by-step project support.

NEEDS

Aligning project outcomes with the company's Infrastructure and Communications technology (ICT) and BMS portfolio.

Vulnerability testing, monitoring, and management of OT systems.

Reducing system exposure to cyber threats.

Ensuring full compliance with the relevant global company-wide Cybersecurity and ICT policy.

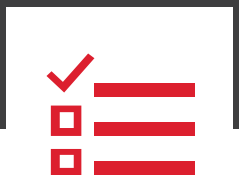
Connecting third-party systems from multiple vendors into one unified network platform.

SOLUTION

OT covers software such as the BMS that control or monitor processes, equipment, or the environment. To help identify potential challenges and risks proactively, the Honeywell team first designed and created a Quality Assurance (QA) environment. The team used mockup and prototype methods throughout the project to help minimize errors and established a Proof of Concept (POC) in one of the buildings to showcase a transparent execution process. By using a global strategy that addresses OT cyber risks, it was possible to create a more robust cyber secure framework for all new deployments.

An audit of the facility's ICT infrastructure and the environment was mandatory. The key risks revealed old operating systems and end-points that were locally managed and maintained, so an Operations and Maintenance (O&M) team was deployed to manage associated activities. Besides engaging with qualified ICT partners during the Vulnerability Assessment and Penetration Testing (VAPT) process, Honeywell also involved its global cybersecurity stakeholders in presenting best practices. A customized process and Standard Operating Procedure (SOP) are now in place to support future facility needs.

Within a tight deadline, the Honeywell team met project expectations and delivered a more robust, end-to-end solution that more broadly covered the integrated network of the facility. These results were achieved thanks to the following cybersecurity services:



CYBERSECURITY ASSESSMENT AND ADVISORY

WHAT WAS INCLUDED

Reviewing your site's OT systems by following global best practice frameworks such as the National Institute of Standards and Technology (NIST) cybersecurity framework. This step helps you identify vulnerabilities and provides visibility over potential issues.

WHAT IT BRINGS

Detailed report

Action plan

Cyber baseline

SECURE CONFIGURATION AND DESIGN

WHAT WAS INCLUDED

We assist you in implementing a securely designed OT infrastructure. Our team delivers cost-effective domain specific configuration that mitigate your facility and OT risks while optimizing the integrity, availability, and safety of your systems.

WHAT IT BRINGS

Architecture and configuration review

Reduced OT risks

Lower associated costs

INCIDENT READINESS AND RECOVERY

WHAT WAS INCLUDED

We provide you with post-incident cyber advisory services, along with assessment and implementation of incident readiness procedures and processes.

WHAT IT BRINGS

Incident response procedure

Reduced downtime

Prepare for Disaster Recovery

BENEFITS

Enhanced user operation management by creating customized SOP, process, and policies to suit the client needs.

A more secure converged network environment with the latest operating system, policies, and patches.

More reliable enterprise endpoint protection.

Compliance with relevant industry frameworks standards (i.e. NIST) and global framesworks for ICT and Cybersecurity policies.

Proven best practices and modern ICT capabilities.

More robust cybersecurity framework model, procedures and reporting methodology.

A more complete solution covering design, deployment, and maintenance stages.

Improved system security with cyber threat monitoring and incident reporting.

Deployed established practices in the cybersecurity space, including third-party systems.

Progressive methodology for data management that helps avoid data leakage and cyber incidents for installed systems and third-party systems.

For more information
www.buildingsolutions.honeywell.com

Honeywell Building Solutions
1985 Douglas Drive North
Golden Valley, MN 55422-3992
Tel: 1-800-345-6770
www.Honeywell.com

Cybersecurity-Bank-CS I 12/19

THE FUTURE IS WHAT WE MAKE IT

Honeywell