Rockwell Automation

Case Studies in Industrial Cybersecurity

Challenges, Solutions and Outcomes Across Industries

Table of Contents

SHARING LESSONS LEARNED

A Message from Rockwell Automation

Dear Readers,

We recognize these are trying times for Critical Infrastructure providers. Amid relentless cyberattacks, complex digital transformation initiatives, and a seemingly unstoppable pandemic, many organizations are grappling with securing operational technology (OT) systems.

OT security has become increasingly important as threat actors have proved they can and will breach IT systems as a stepping stone to infiltrating OT and industrial control systems (ICS). This type of breach, as you'll see, can take down IT systems and Critical Infrastructure, too.

If there's one specific threat that worries business executives, it's the global spike in ransomware attacks. As tensions rise following Russia's invasion of Ukraine, for example, the Cybersecurity and Infrastructure Security Agency (CISA) has warned U.S. state and local governments, aviation and energy sector networks of an increased risk of ransomware attacks from Russia.

Compounding matters, many Critical Infrastructure organizations lack automated threat detection and response capabilities such as continuous monitoring of networks and systems. Other common issues include risks associated with digital transformation, legacy systems and applications, disconnected digital assets, and a lack of centralized network and threat management.

Furthermore, COVID-19 has spawned its own challenges that include the need for secure remote work capabilities, along with periodic operational disruptions and supply chain meltdowns.

Have you ever wondered how businesses deal with these myriad risks? In this digest of Rockwell Automation customer case studies, we explore what has worked for other organizations across a range of industries, including pharmaceutical, life sciences, energy, oil and gas, automotive manufacturing, food and beverage, consumer packaged goods, and manufacturing verticals.

If you're worried about threats to your OT and ICS infrastructure, check out the following success stories. Our experienced teams have helped companies across multiple industries to implement more secure industrial operations. While no infrastructure program is guaranteed to be 100% risk free, there are proven solutions that can substantially lower Critical Infrastructure security risks effectively and efficiently.

Kamil Karmali

Global Manager, Cybersecurity Consulting Services

Rockwell Automation

THE MARKET AT A GLANCE

Cybersecurity Threats Across OT Industries

RANSOMWARE CONTINUES TO DISRUPT

If experience is the best teacher, second-best may be the lessons learned from others in your industry. Organizations breached by internal or external threat actors usually learn valuable lessons about cybersecurity, including how to identify and close vulnerabilities, and how to defend against future attacks.

In this report's sampling of case studies, we'll examine how 10 Critical Infrastructure providers improved security defenses before cybercriminals could swipe passwords and infiltrate networks and applications. But first, we'll preview the current state of cyberattacks and security in six of 16 Critical Infrastructure industries as identified by the Cybersecurity and Infrastructure Security Agency (CISA).

PHARMACEUTICAL AND LIFE SCIENCES

Targeting the Heart of a COVID-19 Response

Pharmaceutical and Life Sciences companies are at the epicenter of the COVID-19 response.

Cybercriminals continue to exploit the pandemic for commercial gain by deploying malware, ransomware, phishing, and URL scams, often using COVID-19 and coronavirus themes as lures. As with other industries, threat actors also attempt to gain entry to new remote access infrastructure for employees working from home.

What's more, nation-state attacks from countries such as North Korea, Russia and China — designed to breach companies developing COVID-19 vaccines, therapeutics, and medical devices — are on the rise with increasing sophistication. Attack goals include industrial espionage, theft of intellectual property, and access to protected patient health information, for examples.

Medical device manufacturers are also the target of threat actors attempting to hack into wearable and implantable health equipment. Some of these devices, such as connected pacemakers and glucose monitors, connect to hospital networks using the internet. Many health industry executives worry that connected medical devices open a gateway to cyberattacks on hospitals and medical facilities, with potentially life-threatening consequences.

Given such high stakes, the Food and Drug Administration, which regulates these devices, has prioritized the need for updates to properly secure them.

86% OF ORGANIZATIONS REPORT LIMITED TO NO VISIBILITY OF ICS ENVIRONMENT.

SOURCE: DRAGOS

OIL AND GAS

Pipeline Security and the Shot Heard 'Round the World

Oil and gas executives are understandably worried about ransomware attacks after the breach of Colonial Pipeline, the largest fuel pipeline in the U.S. Their concern is warranted. The attack shut down some business systems and caused gas shortages across the eastern U.S.

According to Bloomberg, hackers gained entry into the networks on April 29, 2021 through a VPN account, which was no longer in use at the time of the attack, but could still be used to access Colonial's network. And one recent report found that 77% of large U.S. energy companies have at least one leaked password online.

Security incidents among oil and gas companies are also mounting as companies digitize and connect operational technology (OT) systems with Industrial Control Systems (ICS) to centrally manage operations. In the U.S., oil and gas is the third most-frequently targeted sector, behind financial services and manufacturing.

The Colonial Pipeline attack underscores threat actors' ability to breach OT systems, as well as the potentially catastrophic impact of attacks on Critical Infrastructure providers – and in turn, on everyday life for consumers.

AUTOMOTIVE

Rising Connectivity Sparks New Cybersecurity Concerns

In the automotive sector, carmakers and parts manufacturers face soaring ransomware attacks that can endanger the security of converged IT and OT systems. One study found that 49% of leading automakers are highly susceptible to ransomware attacks. In many cases, these assaults start with intrusions into IT systems and then spread to connected OT assets.

In a recent attack on a global automaker, for example, cybercriminals conducted a phishing campaign that implanted ransomware on the company's IT system, which then spread to its OT assets. The attack disabled production plants across the globe and disrupted the company's IT and email systems.

Ransomware isn't the only threat keeping executives up at night. Disruptions from cyberattacks on automotive suppliers have created supply chain snags that have cascaded across industries and geographies, curtailing operations and, in some cases, shuttering entire plants.

CONSUMER PACKAGED GOODS (CPG)

Cyberattacks Rising in Frequency and Cost

Among CPG companies, cybersecurity incidents are rising. More than 40% of CPG manufacturers were hit by a cyberattack in 2020. And the financial consequences of compromise are high and rising. The average cost of data breaches in the CPG sector soared to $3.7 million in 2021, a 42.9% jump over the year before.

Trends expected to drive increased cybersecurity requirements include more use of Internet of Things (IoT) sensors and devices, the growing availability of 5G, and IT / OT network convergence. More devices and operating systems will connect and transmit data across networks, significantly expanding attack surfaces.

Addressing supply chain attacks has also spurred CPG manufacturers to rethink procurement, adjust warehouse space, and reconsider delivery models, as well as reassess the viability of their vendors and suppliers.

FOOD AND BEVERAGE

Ransomware Attacks Grow More Destructive

The industry was weathering tectonic shifts in customer preferences for healthier food and engaging shopping experiences. Younger consumers, for example, tend to demand nutritious foods that are plant-based, locally sourced, and distributed in environmentally friendly packaging. At the same time, cyberattacks on food and beverage businesses were becoming increasingly damaging in terms of costs and downtime.

Then came COVID-19. Food and beverage companies quickly implemented remote work platforms to address new worker safety, security and privacy requirements. Businesses discovered their legacy systems and applications were often incompatible with modern cybersecurity solutions. The need for up-to-date, risk-based security programs became more obvious, especially as attacks increased.

For example, the ransomware assault on JBS, a large Brazilian meat processor, hit plants in the U.S., Canada and Australia. Threat actors encrypted the company's systems and data, then demanded a multimillion-dollar ransom to restore access. JBS paid $11 million. What's more, an estimated 40 additional attacks on food producers occurred in the 12 months preceding the JBS attack, according to the Chicago Tribune.

This type of malware campaign underscores the trend toward targeting F&B businesses that use converged IT and OT systems to better manage production. Without proper cybersecurity planning and controls, this convergence can expose OT systems to a range of sophisticated cyber threats.

Learn from the Success of Others

The following case studies show a wide range of challenges experienced by Rockwell Automation customers. Yet all have elements in common.

The best OT cybersecurity solutions – in terms of quality of protection, speed of deployment and ongoing service that minimizes downtime and defends against cyberattacks – require industrial operations experience.

Look for challenges similar to your own in these stories. We recognize that the insights shared in this digest are intrinsically valuable to understanding the types of solutions that can be deployed to overcome OT threats across various industries.

PHARMACEUTICALS

A Global Pharmaceutical Company Achieves Real-time ICS Threat Visibility and Daily Asset Inventories Across 64 Global Sites

Pharmaceutical companies have long been a favorite target of sophisticated cybercriminals. But the COVID-19 pandemic has intensified the need for a risk-based cybersecurity program, and fast.

One global pharmaceutical manufacturer needed help building a cybersecurity program for its IT and OT systems. Unpatched OT assets were increasing security risks to manufacturing plants, and a lack of real-time visibility into threats to ICS controllers made it all but impossible to detect OT malware.

Compounding risks, the pharma company had not segmented its business networks from its industrial plant networks, nor had it limited traffic and pathways to and from critical manufacturing systems.

Looking to the future, the company knew it needed to educate its teams on good cybersecurity hygiene to create lasting, cultural security improvements.

88% OF U.S MEDTECH LEADERS DON'T THINK THEIR COMPANIES ARE PREPARED FOR A CYBERSECURITY INCIDENT.

SOURCE: IRDETO

WHAT WAS DEPLOYED

After assessing the risks, this pharmaceutical giant partnered with Rockwell Automation, taking significant steps toward maturing cybersecurity protections through network segmentation, and by fortifying endpoint and perimeter security.

At the outset, a three-phase cybersecurity program was quickly designed and implemented.

The first priority involved separating logical and physical networks at 64 global sites to help contain the spread of threats as they hit networks and systems. The company also boosted the security of perimeter devices to impede threat actors, and deployed application "allow lists," to only allow application usage if the applications were pre-approved, to protect endpoints.

Next, the company implemented a suite of threat detection services and implemented USB cleansing to centrally manage and monitor USB media on the OT network, to protect against threats or attacks — from inside and outside the network. The threat detection services also determine normal network behavior that can be used as a baseline, and employ 24/7 threat monitoring capabilities to detect and raise a red flag when anomalous activities are detected. That helps the company identify activities that may pose a risk to its systems more quickly, or before attacks.

OUTCOMES

Rockwell Automation helped the pharmaceutical company design and implement an expanded security strategy across 64 global sites in approximately nine short months. Doing so has improved the company's ability to defend its OT and ICS assets from increasingly sophisticated cyber threats. The company now has real-time, consistent visibility into ICS threats across the global enterprise

BY THE NUMBERS

Quickly building sophisticated defenses against cyber threats

SCOPE

- 9 months deployment
- 64 global sites

SOLUTIONS

- Cybersecurity plan
- Network segmentation
- Endpoint and perimeter security
- Threat detection
- USB media management

LIFE SCIENCES

A Medical Device Maker Modernizes Network Infrastructure to Improve OT Cybersecurity and Enhance Growth

A U.S.-based medical device manufacturer had big plans to ramp up its global production capabilities.

Its growth forecasts led to the requirement for a standardized infrastructure blueprint that could support the expansion of its digital transformation efforts and modernize its OT infrastructure. The company also needed to bolster cybersecurity by segmenting its IT and OT networks.

Over the years, investments in OT had not kept pace with IT, and the company needed to re-engineer
IT and OT systems to strengthen cybersecurity protection for an evolving, and expanding digital enterprise.

Speed was of the essence. The device manufacturer needed to develop and rapidly deploy a centralized cybersecurity and modernization strategy to help protect its expanded networks and digital assets. Yet the company lacked resources to implement new capabilities quickly enough to meet enterprise timelines.

80% OF GLOBAL SECURITY LEADERS SEE RANSOMWARE AS A DANGEROUS AND GROWING THREAT TO PUBLIC SAFETY.

SOURCE: WORLD ECONOMIC FORUM

WHAT WAS DEPLOYED

Rockwell Automation collaborated with the medical device manufacturer to develop a comprehensive plan to assess and redesign networks, and add an Industrial Demilitarized Zone (IDMZ)for seven sites across four global regions.

Next, a standard design blueprint was developed for the organization's virtual infrastructure. The business started by segmenting its IT and OT networks to better secure data that flows between the environments. Another key initiative involved creating a digital security boundary, known as an IDMZ between IT and OT networks. This technology uses network and application security controls to manage and protect the flow of data across zones.

Throughout the 12-month initiative, the company needed line of sight into the precise requirements and costs of automation, as well as network and IDMZ implementation and consistent network design standards. The company worked with several Rockwell Automation ecosystem partners to gain this view and to support implementation, including Panduit for physical installation and cabling and our LifecycleIQ Services business for global deployment of Supervisory Control and Data Acquisition (SCADA) systems.

The firm also implemented a Managed Services program to monitor and manage its networks, data centers and applications.

OUTCOMES

The solution achieved the company's goal of establishing a standard network and IDMZ infrastructure blueprint to support fast, secure growth, along with boosting production capacity. The blueprint provided the right structure for phased implementation for greenfield sites, and can also be used to modernize network infrastructure at existing sites and remotely manage expansion of network requirements.

The medical device manufacturer now has line of sight into its capital expenditures (CapEx) for these requirements, enabling better strategic planning and decisions and ensuring that cybersecurity is addressed as the company grows.

BY THE NUMBERS

Scaling securely with a modern network infrastructure

SCOPE

- 12 months deployment
- 7 global sites

SOLUTIONS

- Network design and blueprint
- IDMZ
- Managed cybersecurity services

ENERGY COMPANY

Natural Gas Storage and Pipeline Firm Tightens Cybersecurity at 62 Compressor Stations and Terminals with Real-time Threat Detection and Asset Inventory Monitoring

As oil and gas companies scramble to avoid rising cyberattacks, many understand the need to deploy a comprehensive cybersecurity program to protect their IT and OT networks.

That was the case with a large U.S. interstate gas pipeline provider. The lack of a unified cybersecurity program left the company's business and IT leaders with, at best, a minimal understanding of current and future threats to equipment, networks, and production uptime. At any given moment, an attacker could infiltrate the company's digital assets without detection, which could disrupt operations and even damage or shut down plants and facilities.

As the company connected IT and OT systems as part of its digital transformation, business leaders recognized the need to get serious about implementing a centralized, risk-based cybersecurity program that would enable the company to quickly detect and respond to cyber threats across networks.

77% OF LARGE U.S. ENERGY COMPANIES HAVE AT LEAST ONE LEAKED PASSWORD ONLINE, LEAVING THEM VULNERABLE TO ATTACK.

SOURCE: THE HOUSTON CHRONICLE

WHAT WAS DEPLOYED

Rockwell Automation helped the natural gas pipeline firm design and deploy the foundation for unified threat protection at 62 North American compressor stations and terminals.

Working with ecosystem partner Claroty, Rockwell Automation designed managed threat detection services with asset inventory monitoring to identify all IT and OT assets on the company's network. Installed base asset inventorying is a critical step for exposing security vulnerabilities and for developing a plan to block internal and external threats, which allows faster response and containment of cyberattacks. The pipeline provider also collaborated with Claroty to implement its real-time threat monitoring solution and define workflows for incident response.

With modern threat detection capabilities, the pipeline provider is now ready to quickly notice and respond to cybersecurity threats in the field and at business locations. It also developed workforce best practices delivering a clear line of sight around evolving requirements.

OUTCOMES

Rockwell Automation helped the company complete the foundation for a modern security initiative in approximately 11 months — a quick turnaround for a complex, but urgent mission. Today, with full visibility into all digital assets on IT and OT networks, the company has improved its security standing and can continuously identify security threats in real time, and rapidly respond to incidents to help lessen the impact of breaches.

BY THE NUMBERS

Putting security in the pipeline

SCOPE

- 11 months deployment
- 62 North Americas sites

SOLUTIONS

- Managed threat detection
- Threat monitoring
- Asset inventory
- Incident response planning

OIL AND GAS

Oil and Gas Provider Reduced Cyber Downtime Risk in a Single Month, Using Real-time Threat Detection and Network Asset Inventory Identification

Cyber threats to oil and gas systems are climbing as threat actors target the energy sector with ransomware and other malware. The Colonial Pipeline attack proved that breaches can severely disrupt Critical Infrastructure services and supplies affecting millions of people and causing significant financial losses.

In parallel, COVID-19 has sped the pace of digitization, along with the need for employees to work remotely, further increasing security risks.

To reduce risks, a multinational energy company needed to strengthen its corporate risk management strategy. A key element included updating OT systems to minimize risks in the event of a cyberattack.

The company also knew it needed to proactively defend its digital assets by implementing a scalable threat detection platform that could rapidly identify vulnerabilities and potential threats, and generate data-driven operational insights to improve decision-making.

The business also needed help with managing costs related to technology obsolescence and modernization, as well as remediating inconsistent solutions engineering into a more unified infrastructure.

79% OF OIL AND GAS COMPANIES REPORT AN INCREASE IN DISRUPTIVE ATTACKS OVER THE PAST 12 MONTHS.

SOURCE: EY GLOBAL STATE OF SECURITY SURVEY 2021

WHAT WAS DEPLOYED

Working with Rockwell Automation, a comprehensive threat -detection program was designed and deployed. The solution identifies a baseline of normal network behavior as well as supplying real-time network asset inventories. The solution then continuously monitors activity to detect and report unusual behavior, before threats become breaches. The threat detection solution also provided a deep understanding of OT systems and network activity for overall improved decision-making.

Working with the energy company, Rockwell Automation and ecosystem partner Claroty implemented threat management solutions for a total of 12 refineries, 3 midstream facilities, 1 SCADA system, and 1 centralized enterprise management console.

49% OF TOP U.S ENERGY COMPANIES HAVE A CRITICAL VULNERABILITY DUE TO OUT-OF-DATE SYSTEMS.

SOURCE: BLACK KITE RESEARCH

OUTCOMES

This oil and gas company now has a unified strategy to protect OT and IT networks from breaches including threat detection services and real time asset inventory capabilities, allowing the company to detect, respond to, and mitigate cybersecurity threats while reducing the likelihood of downtime from cybersecurity incidents, which minimizes business continuity risk.

The solution delivered improved security capabilities in the month after pilot deployment. It currently helps business leaders better understand operational and workforce performance, reduces security team overload and supports data-driven decision-making.

BY THE NUMBERS

Minimizing business continuity risks with enhanced threat detection

SCOPE

- 1 months pilot
- 17 sites
- Ecosystem partner: Claroty

SOLUTIONS

- Threat detection
- Real-time asset inventory

AUTOMOTIVE

How an Automotive Manufacturer Assessed OT Security for Improvements in Record Time

Automotive manufacturers are grappling with multiple challenges as they navigate rapidly evolving product demands and a transforming ecosystem. Amid chaotic conditions, a global automotive manufacturer became worried about its cybersecurity shortcomings.

Specifically, the company was concerned that OT vulnerabilities could allow cybercriminals to slip into IT and OT networks to steal sensitive information, and disrupt operations and production lines. Though the company had recently invested in securing its critical manufacturing environment, leaders nonetheless believed that the networks remained vulnerable to breach. And because a flood of phishing and ransomware attacks have preyed on individual employees, the company knew enhanced threat awareness among employees would help reduce cybersecurity risks to the company's IT and OT infrastructures.

48% OF AUTOMOTIVE MANUFACTURES ARE AT HIGH RISK FOR A RANSOMWARE ATTACK.

SOURCE: BLACK KITE, RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2021, JUNE 2021

WHAT WAS DEPLOYED

Rockwell Automation helped the automotive company assess cybersecurity capabilities using penetration testing - a simulated cyberattack on systems, performed by experts, to identify security gaps.

In this case, the automotive company wanted to determine whether external actors could infiltrate and gain control of IT and OT environments. Thanks to the Rockwell Automation team's OT cybersecurity expertise, the necessary testing services were performed six weeks faster than an average third-party provider.

In fact, within two days, the team discovered that remote-control software had been installed in multiple areas of the factory floor to enable security practitioners to connect quickly. Our cybersecurity experts worked with the company's CIO and CISO to test the application and discovered the ability to connect directly from the public internet to each production environment, bypassing perimeters hardened with firewalls.

In other words, in a two-day penetration test, Rockwell Automation discovered that cybercriminals could gain full control of IT and OT networks and access digital assets and devices including Human Machine Interface (HMI) servers and control systems, confidential manufacturing plans, customer data, security cameras, and even user passwords for Microsoft Office 365 email accounts, including that of the CEO.

OUTCOMES

Penetration testing and assessment helped to quickly identify multiple critical vulnerabilities, exposing access pathways that could allow threat actors to control the manufacturer's assets and production environments. Executive leaders now have a real-world understanding of vulnerabilities and how to better protect their IT and OT infrastructures. The assessment led to Rockwell Automation building a complete protection plan tailored to the automotive manufacturer's needs, based on vulnerabilities discovered during the penetration testing. The automotive business planned to expand security assessments and gap remediation, and to help employees understand the importance of good cybersecurity hygiene.

BY THE NUMBERS

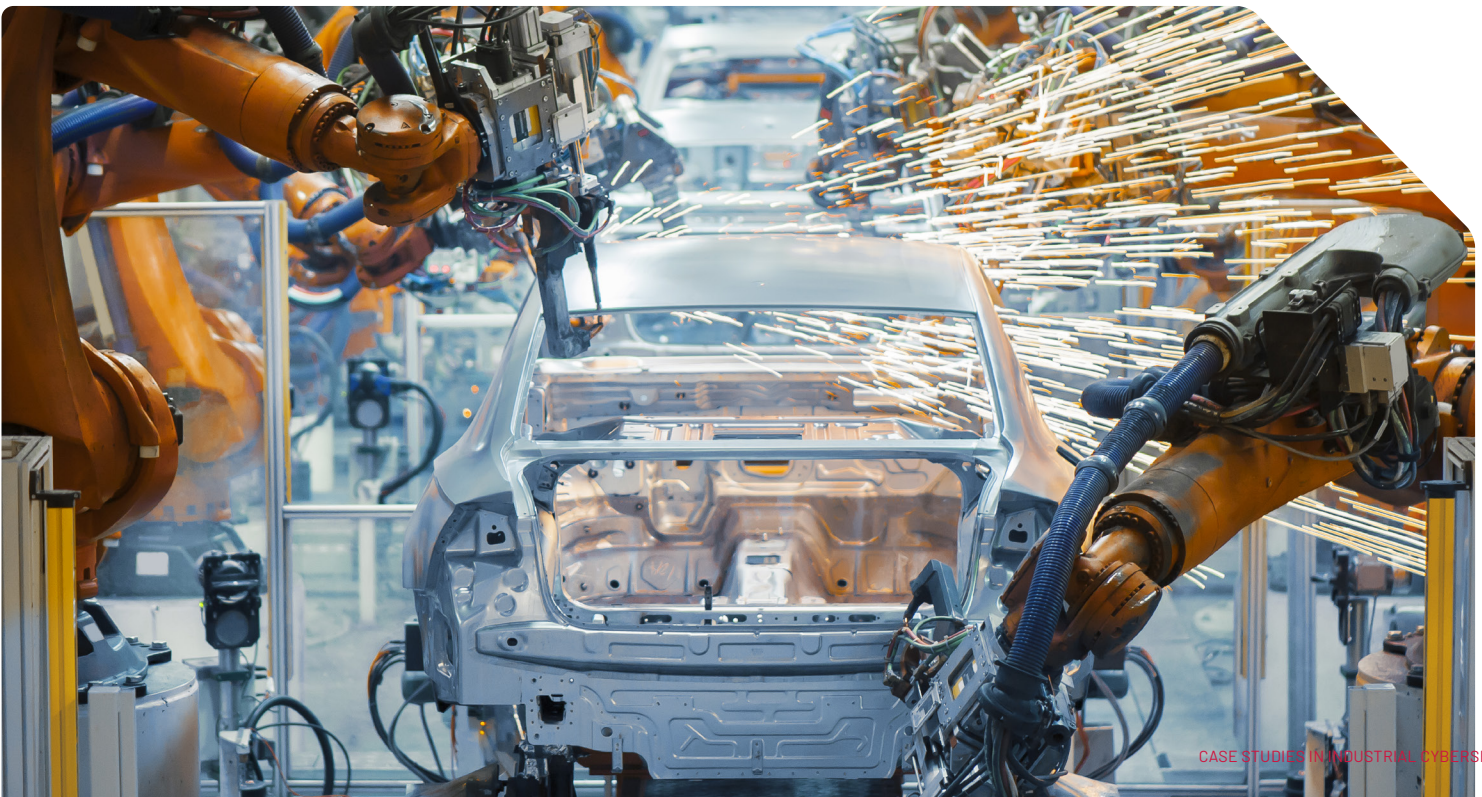
Penetration testing identifies critical vulnerabilities

SCOPE

- 2 weeks
- 6 sites

SOLUTIONS

- Penetration testing



CONSUMER PACKAGED GOODS

A Food Manufacturer Deploys Unified Threat Management across 46 Global Sites, Aligning Cybersecurity among Dozens of Acquired Companies

While some consumer packaged goods (CPG) companies have flourished during COVID-19 — think grocery, food, and health product providers — others have floundered. Yet both face daunting challenges. Cyberattacks are increasingly commonplace and costly, interconnected OT and IT systems can jeopardize industrial control systems, and evolving public-safety requirements demand agility.

To overcome these hurdles, one Fortune 500 consumer food manufacturer needed a clear understanding of cybersecurity vulnerabilities to its OT and IT networks. Complicating matters, the company had acquired dozens of food businesses over the past two decades, each with disparate technology and security ecosystems.

As a result, the manufacturer lacked a centralized, real-time view into the security of systems across its 46 global manufacturing sites. Achieving transparency would require a standard risk-based security strategy and unified threat management capabilities.

43% THE AVERAGE COST OF A DATA BREACH AMONG CPG COMPANIES SOARED TO $3.7 MILLION IN 2021, A 42.9% INCREASE OVER 2020

SOURCE: IBM SECURITY, COST OF A DATABREACH REPORT 2021, JULY 2021

WHAT WAS DEPLOYED

Collaborating with the company's head of cybersecurity and working with ecosystem partner Claroty, Rockwell Automation designed and deployed centralized threat detection services across 46 global manufacturing sites. This helped determine a baseline of network activity and allowed continuous threat monitoring for unusual activity that could indicate cyberattacks, without disrupting operations.

Now, if a breach occurs, a custom workflow helps recover compromised systems and networks. And because employee training is elemental to effective security, a program was implemented to foster an enterprise-wide culture of cybersecurity hygiene.

OUTCOMES

This food manufacturer currently has centralized and unified threat management systems in place to help minimize cybersecurity risks by expanding visibility from IT into the OT environment, detecting and acting on cyber threats before they become breaches. Employees have new cybersecurity awareness resulting from the enterprise-wide training program.

Going forward, the company is positioned to implement consistent cybersecurity programs as it continues to grow through future acquisitions.

BY THE NUMBERS

Centralizing threat detection, minimizing risk to global OT and IT networks

SCOPE

- 46 Global sites
- Ecosystem partner: Claroty

SOLUTIONS

- Threat detection services

FOOD AND BEVERAGE

A Food and Beverage Manufacturer Boosts Cybersecurity and Incident Response, Improves Equipment Effectiveness Score (OEE) by 5%

Following a malware attack that disrupted computing systems and production lines, a global snack foods company needed to strengthen cybersecurity defenses and modernize its network infrastructure across 80 sites worldwide. It had earlier attempted to deploy an Overall Equipment Effectiveness (OEE) platform to help measure and mitigate security risks and improve performance of existing applications. But the initiative sputtered due to incompatibilities among the OEE software and the company's enterprise control layer and network requirements.

The business asked Rockwell Automation to help create a global inventory of its digital assets and modernize its incident response and overarching cybersecurity capabilities.

43% INCREASE IN THE TOTAL AVERAGE COST OF A DATA BREACH IN 2021 AMONG CPG COMPANIES.

IBM SECURITY, COST OF A DATA BREACH REPORT 2021, JUNE 2021

CHALLENGES

Times have been tough in the consumer packaged goods (CPG) segment. No one is a stranger to the last decade's seismic shifts in product and shopping preferences, battered global supply chains, pandemic policies limiting crowd sizes, and the shortage of qualified workers.

Now add the skyrocketing frequency of cyberattacks.

WHAT WAS DEPLOYED

Rockwell Automation collaborated with the company's global director of engineering to assess its networks and help ensure the data needed to measure OEE would be compatible with enterprise networks and applications.

Rockwell Automation then conducted comprehensive network assessments across the company's global facilities and implemented interoperable Industrial Data Centers (IDCs) for remote monitoring and management of digital assets. After an in-depth assessment, our team developed a plan to mitigate network conflicts with the OEE application and implement 24/7/365 remote monitoring and administration by the Rockwell Automation support team.

OUTCOMES

With the new network infrastructure in place, this snack foods manufacturer quickly saw improvements in data accuracy and standardized global reporting. A unified infrastructure, paired with our managed services helped the business decrease downtime, increase data accuracy, and more quickly respond to cybersecurity incidents using service level agreements (SLAs).

Together, these factors helped the food and beverage company boost its overall OEE score by 5%. Even a 1% improvement in OEE can mean a great deal of cost savings on a large production line, and can support the business case for shoring up a company's OT cybersecurity defenses.

BY THE NUMBERS

Improving cybersecurity and gaining higher OEE

SCOPE

- 80% global sites
- 5% improvement in Overall Equipment Effectiveness (OEE)
- Ecosystem partner: World Wide Technology

SOLUTIONS

- Solutions
- Network assessment
- Global asset inventory
- IDC deployment for 24/7 remote monitoring and management
- Incident response

FOOD AND BEVERAGE

A Food and Beverage Company Streamlines and Simplifies OT Cybersecurity with 24/7 Managed Support Services

CHALLENGES

Many manufacturers fail to update legacy systems and software over the years. This can increase the risk of cyberattacks, create operational inefficiencies that chip away at results, and complicate digital transformation efforts.

That's the situation a global food and beverage manufacturer found itself in as it began planning a multi-year modernization project. Three main challenges needed to be addressed. One key goal: to streamline the management of its critical OT systems and integrate new assets that had not been consistently implemented with the aging technologies still in use. Without this integration, the company's workforce lacked the skills to consistently manage the OT systems.

Compounding matters, the COVID-19 pandemic stoked demand for food products. The company's business leaders worried that their technology infrastructure could not withstand the increasing traffic, potentially resulting in downtime and loss of revenue.

The company also needed help implementing secure remote access to protect against rising cybersecurity incidents as more employees and third parties worked from home. Combined, these factors created an unstable and unreliable technology ecosystem that caused unplanned financial losses. The manufacturer needed help implementing consistent, reliable management of its OT digital assets to help ensure reliable uptime amidst the challenges.

WHAT WAS DEPLOYED

The food and beverage company asked Rockwell Automation to help deploy managed services to better protect against cyberattacks, as well as create a stable and efficient operational environment.

Rockwell Automation worked with the company to design an enterprise OT Managed Support Services program that supports all digital infrastructure equipment. Additional solutions were implemented to enable consistent deployment and support for critical applications, software, and infrastructure, as well as 24x7 remote monitoring.

Rockwell Automation also helped the company deploy 19 OT Industrial Data Centers (IDCs) with a continuous threat detection platform to address cybersecurity risks. And to protect home-bound workers, we designed and implemented secure remote access at 40 North American sites.

OUTCOMES

The modernized infrastructure and supporting managed services allow this manufacturer to reduce cybersecurity threats to its corporate and OT networks through 24/7 threat monitoring, while minimizing downtime risks. Consistent deployment and integration of technology assets have helped boost system reliability, and improve application management and plant uptime. Deployment of secure remote access capabilities protects employees, third-party partners and the company's operational infrastructure from cyber risks.

Combined, these initiatives have allowed the company to increase operational efficiencies while reducing costs.

BY THE NUMBERS

Updating legacy systems and gaining powerful cybersecurity protections

SCOPE

- 40 sites
- 19 OT Industrial Data Centers

SOLUTIONS

- Managed support for all digital infrastructure equipment
- OT Industrial Data Centers
- Secure remote access
- 24/7 threat detection

CONSUMER PACKAGED GOODS

CPG Company Undergoes Secure Digital Transformation, Lowering Average Network Response Times by 90%

The seemingly unstoppable COVID-19 pandemic has upended workplace operations, transformed consumer shopping habits, and crippled global supply chains. Compounding matters is a steep rise in the frequency, severity, and cost of cyberattacks. Consider, for instance, that among the 61% of manufacturers reporting a cyberattack in 2021 in one study, 75% sustained system outages.

A side effect of pandemic challenges has been the fast-tracking of digital transformation efforts to meet new challenges like remote work, and the parallel requirement for industrial cybersecurity to protect newly connected operations and networks.

As one multinational food and beverage manufacturer discovered, digital transformation and cybersecurity can no longer be viewed as two separate initiatives, but must be implemented holistically. The company planned to launch a security-centric digitization initiative to take advantage of real-time data generated by its increasingly digital business systems. But it would first need to address technical deficiencies that had accumulated over the years.

The food manufacturer's legacy systems and applications, for example, were incompatible with modern cloud computing and cybersecurity platforms. Its disparate networks and virtual infrastructure couldn't accommodate critical data analytics and artificial intelligence technologies. And inadequate cybersecurity awareness and training programs for employees contributed to a culture of poor security hygiene.

61% OF FACTORIES EXPERIENCED A SECURITY INCIDENT IN 2021.

SOURCE: TRENDMICRO, THE STATE OF INDUSTRIAL CYBERSECURITY, MAY 2021

WHAT WAS DEPLOYED

The CPG manufacturer asked Rockwell Automation to help modernize and unify its IT and OT systems, implement automated monitoring and management of the new network, and update cybersecurity capabilities across 44 sites in North America. It did not want to tap into capital expenditure (CapEx) funding to do so, however.

Rockwell Automation created and deployed a modern cloud-based solution using our Infrastructure-as-a-Service (IaaS) offering. Our team collaborated with the CPG company to design the IaaS network and implement cybersecurity capabilities to include network segmentation, patch management for operating systems, and antivirus solutions. A Rockwell Automation ecosystem partner, World Wide Technology, managed the delivery of hardware for the initiative. All network and compute infrastructure were then migrated to a managed service in OT.

The company also deployed Rockwell Automation's TechConnectsm Support and Application Support services for improved 24/7 help desk support for applications and infrastructure, and to dispatch on-site field labor for 'hands-on keyboard' support. While service level agreements (SLAs) mandated a response to IaaS alerts in 10 minutes or less, actual response times averaged just 3.5 minutes.

OUTCOMES

This secure digital transformation solution closed large cyber-risk gaps by implementing a modern network infrastructure using Infrastructure-as-a-Service offering, as well as effective OT patch management – a notoriously complex security requirement to solve – and antivirus safeguards.

Using the Rockwell Automation's Application Support service, the company improved response time for critical alarms and alerts by 90%, which in turn diminished downtime. Funding for the initiative came from the company's operating expenditures, which enabled it to fund digital transformation without tapping into CapEx reserves. The globally-supported, services-ready support model helped address staffing shortages for skilled IT and cybersecurity workers in their newly digital operations, and prepared the company for future scaling.

BY THE NUMBERS

Secure Digital Transformation, 90% improved response time

SCOPE

- 44 North American sites
- 10-minute IaaS SLA decreased to an average of 3.5 minutes
- Ecosystem partner: World Wide Technology

SOLUTIONS

- Infrastructure-as-a-Service (IaaS)
- OT patch management
- Antivirus
- TechConnectsm support and application support

CHEMICAL

Chemical Company Provides Employees with Secure Remote Access to Control System Handling for 8,000 I/O Points during Pandemic

CHALLENGES

As COVID-19 persists, a significant number of people continue to work from home. Biofuel companies are no exception.

One South American producer of ethanol, bioenergy, and livestock feed needed to implement secure remote access to the company's IT and OT networks. A top priority was implementing secure access for a greenfield initiative with remote suppliers. The biofuel company also needed to work around mandates for reduced travel while enabling audits of all remote interactions with the industrial control system (ICS).

WHAT WAS DEPLOYED

The biofuel company partnered with Rockwell Automation to design and deploy security solutions with complex power supply options.

The first priority was the greenfield project. Rockwell Automation provided consulting to help the company understand the complex array of power supply options that would be appropriate to meet project goals. One selected option was Intelligent Packaged Power (IPP) with medium- and low-voltage power equipment, integrated into the company's Distributed Control System (DCS).

28% GLOBAL DEMAND FOR BIOFUELS IS FORECAST TO GROW BY 28% BETWEEN 2021 AND 2026.

INTERNATIONAL EMERGENCY AGENCY, RENEWABLES 2021 ANALYSIS AND FORECAST TO 2026, DECEMBER 2021

Rockwell Automation then helped the business improve centralized security information monitoring, implementing an Industrial Data Center (IDC) solution and 24/7 remote monitoring and administration capabilities for the virtual environment. Our team also designed and implemented an Industrial Demilitarized Zone (IDMZ) to securely isolate the company's business networks and industrial control systems.

Secure remote access and configuration capabilities were also critical, given COVID-19 travel and social distancing restrictions. Doing so allowed the biofuel company to monitor remote operator interactions with the ICS, as well as audit all remote interactions with a key supplier located 1,243 miles away from the site. This approach will also be deployed in future greenfield sites.

OUTCOMES

Using lifecycle services from Rockwell Automation, paired with deployment of an IDMZ and secure remote access, the company completed its greenfield project requirements while reducing cybersecurity risks to corporate and OT networks. The initiative also simplified control and monitoring of OT and ICS remote-access sessions, increased system reliability, improved workforce efficiency, and improved system support coverage with 24/7 remote monitoring.

Rockwell Automation's team also helped the biofuel business enhance employee safety protocols for pandemics — present and future.

BY THE NUMBERS

Deploying secure remote access during the pandemic

SCOPE

- 2 sites
- Ecosystem partner: Claroty

SOLUTIONS

- Threat detection services

Rockwell Automation: Securing What the World Relies On

Rockwell Automation provides a range of industrial security solutions and services to help you manage threats and boost the resiliency of your OT and IT operations. Our experts can design a robust and secure network infrastructure, while defending against threats and rapidly responding to incidents with 24/7 monitoring In addition to deep expertise and knowledge of the latest best practices, we bring production operations wisdom derived from more than 100 years in industrial automation.

Our worldwide locations enable customers to apply consistent cybersecurity protections on a global scale across multiple sites, with logistics as finely tuned as you'd expect from the industry leader in industrial automation.

Resources to help you get started

- Learn more about common OT cybersecurity attacks. Watch the Automation Fair® conference session presentation: Top 10 Cybersecurity Attacks in OT.
- Take our Cybersecurity Preparedness Assessment and receive a custom report, benchmarked against original survey respondents. See how your organization compares by industry, company size and region.
- Talk to a Rockwell Automation expert and learn how we can help you gain the right OT cybersecurity program to protect your industrial operations.

Rockwell Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-AP001A-EN-P-May 2022