Rockwell Automation

A Rockwell Automation Workbook

Build the Right Business Case for Your Industrial Cybersecurity Program

Winning Leadership Support for OT Cybersecurity Initiatives

Most leaders understand the importance of protecting industrial operations from cyberthreats. Yet leaders must continually balance investments in cybersecurity against other organizational priorities and initiatives.

Added to the balancing act, specialized knowledge of industrial control systems (ICS) and operational technology (OT) may be limited among organizational leaders, along with insights into modern cybersecurity approaches, tools and processes needed to protect ICS/OT systems.

IT leaders may see that OT resources are less vulnerable to attack when compared to digital IT resources including networks, servers, and databases. That's because OT resources historically have been isolated from IT networks, and have had few, if any, external connections that would give an adversary an avenue for attack. IT leaders also believed the risk of an attacker targeting industrial systems was low, rooted in the belief that there's little value for attackers in OT environments – such as no personally identifiable information (PII) or credit card numbers to steal.

Today, however, plant operations are increasingly digital and interconnected, silently introducing new risks for businesses. And unfortunately, today's attackers know that disrupting plant operations can be astronomically costly to any organization. They have learned that organizations have a high willingness to pay ransom fees if it means restoring operations sooner.

The Need for Realistic Risk Identification

In parallel, geopolitical heat is rising, with nation-states actively looking at critical infrastructure as potential cyberwarfare targets. A successful cyberattack on industrial systems can have devastating consequences, beyond production downtime, equipment damage, and financial losses. Such an attack can impact operator safety, and even disrupt life-sustaining services such as food, water, transportation, healthcare and energy.

Building a business case for industrial cybersecurity can help leaders understand the risks and benefits of investing in cybersecurity measures for OT environments. Quantifying the potential impact involves identifying vulnerabilities, or the likelihood of a cyberattack, and understanding that it's typically less expensive to invest in risk reduction ahead of time. Ultimately, the right cybersecurity business case will support an organization's journey to modernizing OT cybersecurity.

This not only helps leaders to prioritize their investments intelligently, but arms them with the information they need to justify and evangelize the project with key stakeholders, such as the organization's board of directors.

83%

of surveyed Critical Infrastructure organizations said they experienced at least one OT security breach in the prior 36 months.[1]

5 days

Average system outage period due to cyberattacks in the manufacturing industry.[2]

Building Blocks of an Industrial Cybersecurity Business Case

In its most basic form, a business case is a simple document that lays out the costs associated with a proposed investment along with projected benefits, demonstrating an associated return on investment (ROI).

When it comes to building a cybersecurity business case, quantifying costs and benefits can be challenging. Many of the benefits come in the form of reduced risk and cost avoidance. Also, the costs of implementing a new solution may need to be spread across a number of different departments, including IT, OT, security, plant operations, human resources, finance and safety.

Taking a methodical approach to making a cybersecurity business case can help translate complex and subjective concepts into quantifiable values, making it easier for leaders to more accurately determine risks, costs, and to prioritize cybersecurity among competing initiatives.

A cybersecurity business case can contain the following sections:

Business Case Sections	Section Contents	See Page
Problem statement and analysis	Current situation, risk analysis. May include a formal third-party risk assessment.	5
Proposed solution	Overview of proposed solutions; why it's the best set of solutions for the organization.	7
Organizational outcomes	Quantified estimates of value from reducing the risk of a successful cyberattack, including change management criteria, business impact analysis or vendor risk management requirements.	8
Cost breakdown	Review of proposed solution costs across people, processes and technology categories.	11
Return on investment / value	Value of reducing cybersecurity risk compared to the costs of the proposed solution.	13

Now let's examine each of these sections in detail, along with example content.

Problem Statement and Analysis

A business case starts with an overview of the problem that a proposed project is expected to resolve. The problem statement typically includes a summary of the current state, an analysis of root causes, and an overview of business objectives that the project should accomplish.

When it comes to industrial cybersecurity, there's no shortage of challenges for OT teams to address, from cybercriminals and nation-state threat actors to hacktivists and insiders. Common drivers for cybersecurity investments include:

- **Increased cybercrime, especially ransomware**. While many leaders may see cybercrime as primarily an IT issue, cybercrime poses an increasingly significant threat to OT environments, leading to unauthorized access, downtime, and the potential for large-scale disruption.

- **Cybercriminals** may target industrial systems to extort money, steal intellectual property, or more often than not, to disrupt operations. The trend toward large-scale, nation-state driven disruptions is partly driven by digital transformation especially broader and deeper connectivity between IT and OT environments. As industrial systems become more complex, interconnected, and interdependent, it's no longer feasible to protect the OT environment with a simple air gap. Increased connectivity with IT systems, the cloud, third-party vendors, and 5G networks opens an entirely new set of risks to OT networks.

- **Increasing regulation**. Industrial organizations face heavy regulation from various sources, which vary based on country, region, and industry. Fines can be stiff for organizations out of compliance. For example, one year after Colonial Pipeline was hit by a well-publicized ransomware attack, the U.S. Department of Transportation recommended a fine of nearly $1 million, on top of the already high costs Colonial Pipeline paid due to days of downtime and recovery efforts.

87%

Ransomware attacks against industrial systems increased 87 percent in 2022.[3]

29%

of industrial organizations reported experiencing a ransomware attack in the last 2 years.[4]

89%

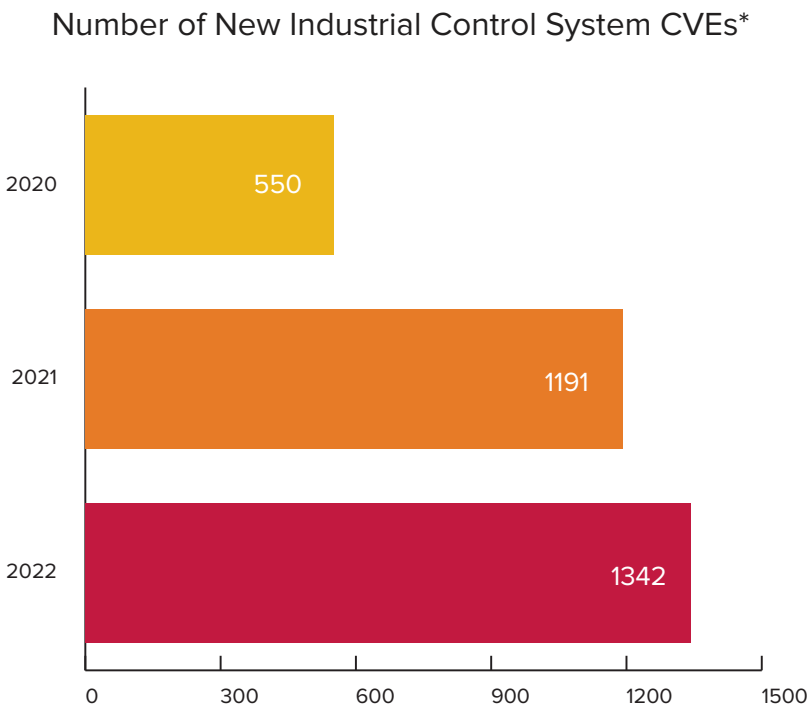
of industrial organizations have had their supply chains disrupted due to cyberattacks.[5]

Problem Statement and Analysis *continued*

Regulation	Affected Industry
North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)	North American electric power utilities
Network Information Security Directive 2 (NIS2)	European Operators of Essential Services
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)	U.S. Critical Infrastructure sector providers
Defense Federal Acquisition Regulation Supplement (DFARS)	U.S. defense contractors
Health Insurance Portability and Accountability Act (HIPAA)	Medical device manufacturers and other organizations that deal with healthcare information
Title 21 of the Code of Federal Regulations (21 CFR Part 11)	Industries regulated by the U.S. Food and Drug Administration (FDA)
H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation (CFATS)	Chemical facilities
United Nations International Treaty	In development now, this treaty focuses on data protection and cyber resilience
NIST Cybersecurity Framework	A global framework for organizational cybersecurity
Cybersecurity Maturity Model Certification (CMMC)	A U.S. Defense Department cybersecurity requirement
MITRE ATT&CK	A foundation for the development of threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community
Trusted Information Security Assessment Exchange (TISAX)	An assessment and exchange mechanism for information security in the automotive industry

A sampling of cybersecurity regulations by industry

Problem Statement and Analysis *continued*



This chart depicts the growth of common vulnerabilities and exposures (CVEs).[7]

- **Skyrocketing vulnerabilities.** Security researchers and vendors continue to disclose new ICS vulnerabilities at an increasing rate each year. The number of U.S.-based threat actors dedicated to attacking industrial organizations has grown by 35% over the past year, driving an 87% increase in breaches over the same period.[6] These vulnerabilities are challenging for defenders to handle not only because of their volume, but also because of the complexity involved in remediating them. While vulnerabilities in IT environments can often be patched relatively quickly, in OT environments there are significant challenges, including warranties that mandate long acceptance testing procedures, and limited maintenance windows.

Example Problem Statement

Throughout this workbook, you'll find brief examples showing how the guidance might be put into practice for a real-world industrial organization.

> "Global Manufacturing Inc. (GMI) is experiencing a significant increase in attempted ransomware attacks, placing the OT environment at high risk of unplanned downtime and data loss.
>
> Over the last 12 months, the number of ransomware-related security alerts has increased 80%. Most of these attacks are targeting IT systems, however the increased connectivity between IT and OT environments within GMI has resulted in the exposure of industrial systems to these cyberthreats.
>
> Risks in the manufacturing plants are especially high due to a large number of legacy systems with unpatched vulnerabilities. In some cases, these systems are no longer receiving security patches from their respective vendors. In other cases, deploying patches requires going through a lengthy regulatory validation process, and patching has been deferred." ”

Proposed Solution

Next, we will introduce the proposed solution to resolve the problem. A strong cybersecurity business case should include an overview of solutions that may have been considered, and an analysis of why the proposed solution is the best one for the organization. The solution description should not only describe the new technology or service that will be deployed, but also provide an overview of the operational model and integration points with existing technology and processes. Describing the complete solution will give leadership a full view of how the new solution will fit in with the existing technology stack, helping to build confidence in a smooth deployment.

Example Solution

> "The GMI team is proposing a project to reduce the risk of ransomware in the manufacturing plants by improving network segmentation and filtering across the OT environment.
>
> Network controls are the most effective way to reduce risk in the current GMI OT environment. Endpoint security controls that are used throughout the GMI IT infrastructure are not feasible in the OT networks, due to the wide range of embedded systems and unsupported OSs.
>
> The proposed solution will consist of a set of industrial network firewalls deployed to tightly control ingress/egress traffic to the Plant DMZ (Purdue Level 3.5), Plant Operations LAN (Purdue Level 3) and Plant Control LAN (Purdue Level 2). Implementing tight ingress/egress controls at these layers will help ensure that no unauthorized network traffic can cross layer boundaries, effectively protecting at-risk systems. The proposed solution also helps to improve GMI's adherence to best practices in industrial cybersecurity as laid out in IEC 62443.
>
> The firewalls will be deployed by the chosen vendor during regularly scheduled maintenance windows, minimizing downtime. After receiving proper training, the solution will be maintained by the GMI security engineering team, and all alerts will be integrated into existing GMI security operation center (SOC) workflows."

For complex implementations – spanning multiple global sites or deploying a full NIST Cybersecurity Framework program over multiple years, for example – the proposed solution might be to begin a Phase 1 project with parallel deployments of risk and vulnerability assessments, threat detection and incident response processes, while also planning out the remaining project phases.

Organizational Outcomes

Now it's time to run the numbers. The foundation of a cybersecurity business case lies in providing an understanding of the benefits to be derived from a proposed investment. The biggest benefits from cybersecurity investments come from avoiding costs and impacts associated with a breach, including:

- **Reduced downtime**. One of the biggest benefits of cybersecurity investments for OT environments is the reduction of downtime associated with cybersecurity incidents. The costs of downtime in industrial settings can be significant, particularly when you consider the costs of lost production, delayed deliveries, spoilage, and idled workers.

  As an example, in February 2022, a global automaker was forced to shut down operations across 14 plants due to a cyberattack on a key supply chain partner. The shutdown resulted in a reduction of approximately one third of the automaker's global manufacturing capacity, representing 13,000 cars per day and hundreds of millions of dollars. Actual costs of unplanned outages vary depending on business size and industry. Estimates range from as much as $8,000 or more per hour for a small-to-medium business, up to $1M+ per hour or more for a large industrial organization.[8]

  Considering that it often takes several days or even weeks for teams to recover from a cybersecurity incident and return to normal operations, it's easy to see how preventing an incident can result in millions of dollars in cost savings.

$2M

Average cost of 1 hour of unplanned downtime in the automotive sector.

$500K

Average cost of 1 hour of unplanned downtime in the oil & gas industry.[9]

- **Avoidance of incident response and recovery costs.** The costs of incident response and recovery for a cybersecurity incident in industrial environments can be substantial. The first step in incident response is to investigate and analyze the incident to determine its cause, scope, and impact. This may involve hiring external cybersecurity experts, conducting forensic analysis of affected systems, and reviewing logs and other data to identify the source of the attack.

  Once the investigation is complete, the next step is to remediate the affected systems and restore normal operations. This may involve patching vulnerabilities, restoring backups, and conducting system testing and validation to confirm that all systems are functioning as expected.

  Additionally, in the case of ransomware incidents or data theft, it's common for threat actors to demand ransom payments to restore access to encrypted data, or to prevent sensitive information from being publicly disclosed. While experts agree, it's best not to pay ransom money to criminal gangs, some organizations choose to do so because it may be their fastest and most cost-effective path to restoring operations.

- **Avoidance of regulatory fines.** Governmental or industry organizations may levy fines on organizations that fail to meet security standards or policies. These fines can be issued for a variety of reasons, including data breaches, poor security practices, and compliance failures. Depending on the severity of the breach or violation, the fines can range from thousands to millions of dollars.

  In recent years, there has been an increase in regulatory fines for cybersecurity violations, as governments and regulatory bodies seek to hold organizations accountable for data breaches and other security incidents. This trend is likely to continue as cybersecurity threats evolve and grow more sophisticated.

$500K

Most industrial organizations paid an average of $500K or more in ransom.[10]

$986K

Civil penalty imposed on Colonial Pipeline by U.S. Department of Transportation after the 2021 ransomware incident.

Other outcomes of cybersecurity investments include:

- **Strategic differentiation**. As cyberattacks become more prevalent, customers are increasingly aware of the risks that come from doing business with third parties. Having a strong cybersecurity program can set an organization apart from competitors, especially for customers in highly regulated industries such as healthcare, government, and energy.

- **Health, safety, and environmental factors**. In the industrial sector, a cybersecurity incident may cause more than outages for digital systems. Such an incident can also have significant impacts in the physical world, including damage to physical infrastructure, environmental damage from chemical spills or contamination, and threats to human safety.

- **Reduction in cybersecurity insurance costs**. Improvements in cyberdefenses make organizations less risky for insurers, which may be reflected in lower premiums or improved terms and conditions.

Outcome Driven Metrics: The table below summarizes the estimated benefits GMI expects to see as a result of the proposed network segmentation project:		**Estimate Your Organization's Potential Outcomes Below:**
Estimated number of cybersecurity incidents avoided:	1 incident/year	
Estimated costs for downtime for a GMI plant:	$50,000/hour	
Expected plant downtime for a cybersecurity incident:	36 hours	
Calculated savings for downtime due to avoided cybersecurity incidents:	$1.8M/year	
Estimated savings for incident response and recovery:	$200,000/year	
Estimated savings for regulatory fees:	$100,000/year	
Total estimated annual benefits:	**$2.1M/year**	

Cost Breakdown: Map Out the Costs

Once the benefits of a cybersecurity investment are well understood, it's time to turn our attention to the costs.

To help leaders make informed decisions, it's important they understand not only the up-front costs associated with a proposed project, but also the ongoing operational costs to be incurred over time.

A typical cybersecurity business case will lay out the costs in a number of different categories:

- **Technology costs**. Any project that introduces new security controls or services into the environment will likely have costs associated with purchasing the underlying technology or service. These costs are typically easy to get from your technology vendor, and may include one-time costs, such as hardware and software licenses, as well as recurring annual costs, such as SaaS subscription fees.

- **Deployment costs**. Before an organization can begin to realize the value of their investment, the proposed solution must first be properly installed and configured. The business case should account for hard costs, such as consulting and training fees, as well as soft costs associated with deployment, such as the labor required to deploy software and hardware, integrate it into existing technical and business workflows, and any planned downtime needed to complete the deployment.

- **Solution maintenance**. Few solutions are truly "set-and-forget." Most solutions will require ongoing maintenance to ensure they continue to operate efficiently, and cybersecurity especially needs ongoing updates as the threat landscape continuously evolves. Vendors typically charge an annual support fee of 15%-25% to provide ongoing support and updates. In addition, local support staff will be required to deploy security patches and software updates in a timely manner, monitor the health of the solution to ensure it is operating properly, and tune policies as necessary to optimize protection.

- **Solution monitoring**. Finally, there are costs associated with actually using the new security solution in a production environment. Many security solutions generate alerts that should be reviewed by staff in a security operations center (SOC). The SOC staff must integrate the new alerts into their existing workflow, to triage, investigate, and respond to any emerging cyberthreats. SOC-as-a-Service, or managed SOC services are available and often desirable given cybersecurity staff shortages worldwide. If a managed SOC approach is preferred, use this pricing model instead for solution maintenance estimated costs.

Example Costs: The table below summarizes the anticipated costs GMI expects to see as a result of the proposed network segmentation project:		**Estimate Your Organization's Potential Costs Below:**
Assumptions		
IT engineering FTE cost:	$150,000/year	
SOC staff FTE cost:	$175,000/year	
One-Time Costs		
Hardware and software:	$350,000	
Professional services (installation and configuration):	$50,000	
Administrator training:	$15,000	
Total one-time costs:	**$415,000**	
Annual Recurring Costs		
Vendor support:	$70,000/year	
Solution maintenance: 0.5 IT engineering FTE	$75,000/year	
Solution monitoring: 1 SOC staff FTE	$175,000/year	
Total annual recurring costs:	**$320,000/year**	

Calculate Return on Investment

Armed with data on solution costs and benefits, it's a simple matter to perform a cost-benefit analysis. This typically starts by calculating the return on investment (ROI). The ROI provides a simple, at-a-glance metric that shows leaders the value to be realized from a cybersecurity investment.

First, consider the time frame for an ROI calculation*. Since the costs likely include some up-front expenses (for example, hardware costs, software licensing, and deployment costs) and recurring costs (such as SaaS subscriptions and maintenance) it's often best to perform ROI analysis over a period of at least three years to provide a complete picture of the value to be derived over time. ROI is typically shown as a percentage, and can be calculated using the following formula:

$$ROI = \frac{(BENEFITS - COSTS)}{(COSTS)} x100$$

This number should not be viewed as a hard dollar return. Much of the benefit of reduced risk and anticipated cost avoidance, which are derived from overall historical trends and averages. Instead, an ROI calculation should be seen as a measure of how much risk can be reduced for the specified expense, and be stated as value.

Example Return on Investment Calculation: The table below summarizes the anticipated costs GMI expects to see as a result of the proposed network segmentation project:		**Calculate Your Organization's Expected ROI Below:**
Estimated cost avoidance/value year 1	$2,100,000	
Estimated cost avoidance/value year 2	$2,100,000	
Estimated cost avoidance/value year 3	$2,100,000	
Total 3-year benefits:	**$6,300,000**	
Deployment costs	$415,000	
Operating costs year 1	$320,000	
Operating costs year 2	$320,000	
Operating costs year 3	$320,000	
Total 3-year costs:	**$1,375,000**	
$ROI = \frac{\$6,300,000 - \$1,375,000}{\$1,375,000} x\ 100$		
3-year value from investment:	360%	

* For simplicity, we ignored the time value of money in our calculations. A more sophisticated analysis would account for the fact that, due to inflation and other factors, a dollar in year 1 is worth more than a dollar in year 3. This may change the overall calculation by a few percentage points, but should not affect the broader conclusion.

Presenting Your Case

Completing a cybersecurity business case is just the beginning of a larger decision-making and implementation process. Armed with a well-documented problem, solution, benefits, and costs, it's time to bring the business case to leaders, who will be well equipped to evaluate the business case based on their own perspectives and priorities.

Ensure you have the right presenters and stakeholders invited to your presentation. Often in industrial cybersecurity that means including key roles from both IT and OT. Prepare for tough questions and rehearse in advance. In some cases, you want experienced cybersecurity consulting experts from outside the organization to help answer questions based on their expertise in prior implementations.

Rockwell Automation: Securing What the World Relies On

Need help? Rockwell Automation is the worldwide leader in industrial automation and industrial cybersecurity, with more than 100 years of experience helping organizations of all sizes to transform. Rockwell Automation can bring recommendations and best practices that are tailored to your business, based on experience deploying simple to highly complex cybersecurity implementations across the globe. We can help to develop a security strategy that works for you.

Learn More

Watch this video demo of a simulated attack and response for insights on how precious minutes and seconds of downtime can be saved with modern cybersecurity protections in place. Then check out Rockwell Automation's free preparedness assessment tool to help gauge your organization's industrial cybersecurity readiness and provide useful statistics to better support a Cybersecurity Business Case.

Or contact Rockwell Automation to speak to an industrial cybersecurity expert today.

Footnotes

[1]Skybox Security: https://www.skyboxsecurity.com/wp-content/uploads/2021/11/OT-research-report-skyboxsecurity-102521.pdf
[2]Trendmicro: https://www.trendmicro.com/en_us/research/22/j/manufacturing-cybersecurity-trends-threats.html
[3]Dragos: https://www.dragos.com/year-in-review/
[4]Dragos: https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en
[5]Trendmicro: https://resources.trendmicro.com/IoT-survey-report.html
[6]Dragos: https://hub.dragos.com/rockwell-automation/ics-cybersecurity-year-in-review-executive-summary-2022
[7]Synsaber: https://14520070.fs1.hubspotusercontent-na1.net/hubfs/14520070/Collateral/SynSaber_Industrial-CVE-Retrospective_2020-2021-2022.pdf
[8]Pingdom: https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/
[9]Siemens: https://www.siemens.com/global/en/products/services/digital-enterprise-services/analytics-artificial-intelligence-services/predictive-services/senseye-predictive-maintenance.html
[10]Dragos: https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en

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-SP022A-EN-P-June 2023