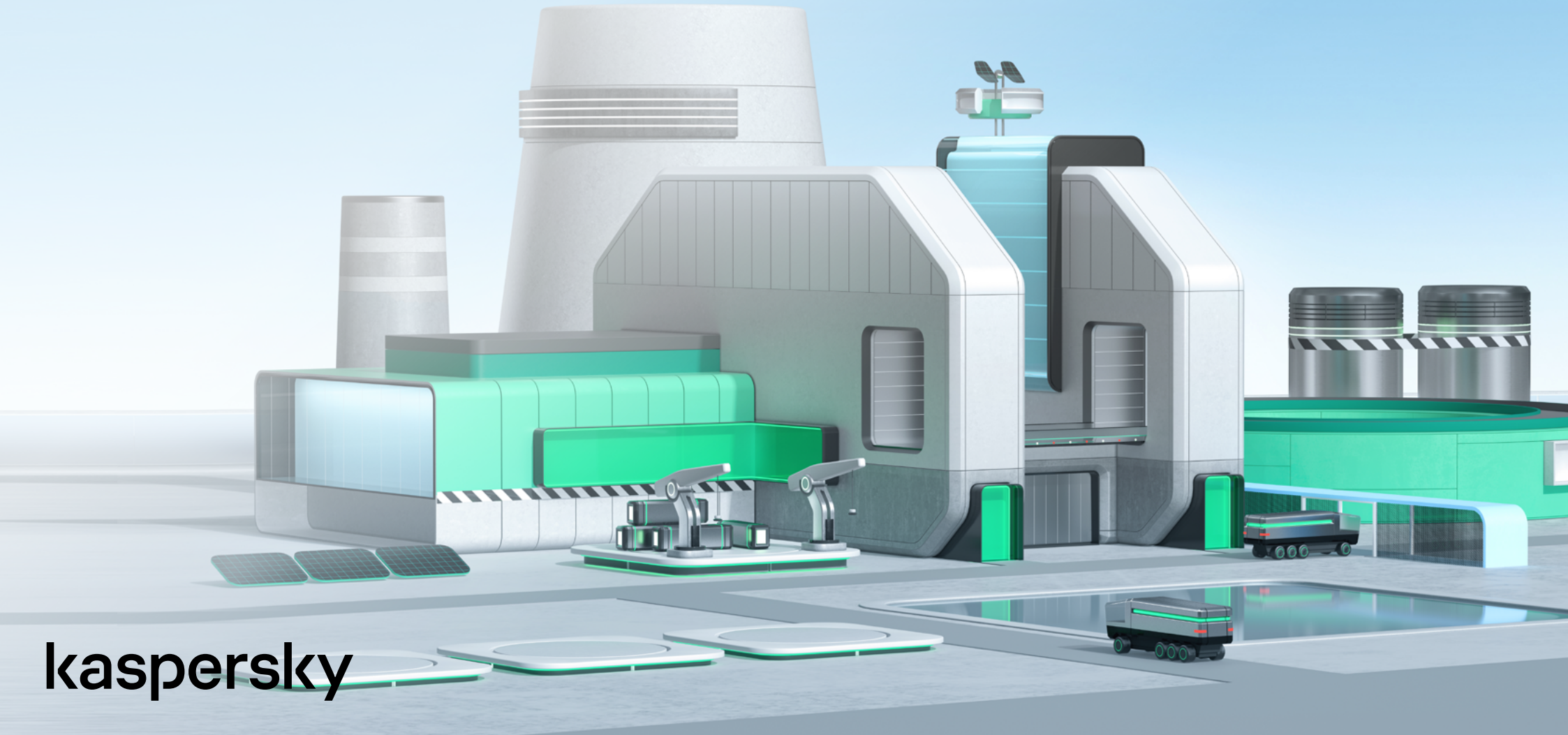
CISO guidebook on OT cybersecurity value: key considerations to justify your investment



kaspersky

Operational continuity, safety, and physical system and process availability enable industrial organizations to generate profit, avoid losses and maintain their reputation. Security, however, should not be framed as a disparate cost center but as a pillar of enterprise risk management. By aligning security initiatives with the goal of protecting these physical and operational investments, you can demonstrate value in terms that resonate with executive leadership.

The cost calculator and guidelines in this document help to demonstrate, justify and realize the tangible value of cybersecurity initiatives to senior management and other key business stakeholders.

A fundamental challenge is the persistent gap in risk tolerance between security teams and executive management. The former is tasked with minimizing it, while the latter must balance it against business objectives and viability – often accepting levels of exposure that make their counterparts uncomfortable. This is not negligence; it's a core function of their strategic role.

Translating threats into business impacts and presenting actions in terms of risk and reward is essential. Executives are wired for strategy, not technical deep dives, and their focus is profitability. To gain their buy-in, speak their language: frame technical challenges as clear risk assessments. Remember, their objective is not to minimize exposure but to make informed decisions that drive profit and growth while minimizing potential loss.

The proposals must demonstrate an understanding of the bigger picture, showing how security management supports the broader business strategy.

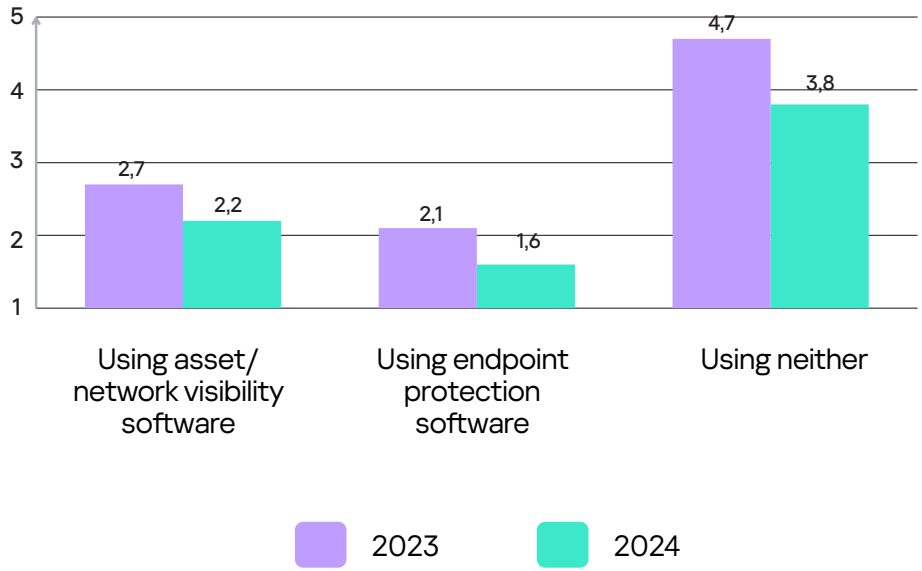
OT cybersecurity is a diverse market that can help you minimize the costly repercussions of a breach. There are many different costs and variables that impact the savings an OT cybersecurity solution can provide, such as the number of breaches prevented, the time and cost associated with remediating breaches and the cost of unplanned downtime.

Consider the below points when justifying your expenditure on OT cybersecurity solutions.

1. The number of cybersecurity breaches that affected operations for the past year

Use your organization's historical data (or check our calculator webpage data) to see how many cybersecurity breaches affected your organization (or those of similar stature) to calculate the probability of such breaches given today's threat landscape. The VDC report[1] contains data on breaches for those who use asset/network visibility and endpoint protection solutions versus those who use neither. If your specific sector isn't covered, the research still provides broad statistics that might be helpful in benchmarking:

Number of cybersecurity breaches that affected organizations' operations in 2023 and 2024



1 Analysis based on VDC's market research and a survey of 250+ OT/IT professionals familiar with their organization's OT cybersecurity practices across multiple industrial sectors including energy and utilities, transportation and logistics, and manufacturing sub-sectors such as chemicals and pharmaceuticals, among others. Download the full report: Securing OT with purpose-built solutions

2. The costs that can result from a cybersecurity breach

Distribution of costs from cybersecurity breaches according to VDC Research:



22%
Incident response

Emergency repair crew

This is the bill for the outside/inside experts you had to fly in. The analysts who figured out how the hacker broke in, what they broke and how to kick them out. This includes their fees, your lawyers and the consultants helping you talk to customers about the delay.

This is pure, unplanned expense. It's money you're spending just to understand the mess and start cleaning it up.



19%
Lost revenue

Missed shipments

The downtime on Line X resulted in a delay in production, which caused a missed shipment deadline for the largest customer. This led to a fine for violating contract terms. Worse, the next contract was awarded to a competitor due to the loss of confidence in the company's reliability.

This is lost sales and lost future business. It's a direct hit to your top line – the revenue you were counting on that simply won't happen.



17%
Unplanned downtime

Idle line cost

Line X was down for 24 hours, yet the company still paid the line operators, maintenance crew, and supervisors. The lights were on, the robots were drawing power, but nothing was being produced. These are the direct costs of fixed overheads and labor during a production halt. It's burning cash with zero output, which can quickly escalate into significant revenue losses.

VDC Research estimates that cybersecurity breaches most commonly cause unplanned downtime lasting anywhere from four to 24 hours.



17%
Equipment/property repair or replacement

Retooling and rebooting

A malicious actor has altered the logic of the robotic production line programmable logic controllers (PLCs) and corrupted your process control system workstations. You had to restore every machine and PLC program from backups, followed by a full production line checkup and secondary startup.

This is the cost of getting your tools back to a working state – and it's close to the cost of initial production line configuration.



12%
Ransom payment

Shakedown

This is a straight-up payment to a criminal. It's a gamble to try to reduce the other costs, like downtime or loss of WIP inventory. It's a business decision, not a technical one.

Kaspersky urges all ransomware victims, whether large or small organizations, not to pay the ransom demanded by criminals.



12%
Loss of WIP inventory

Spoiled batch

When the system crashed, the robotic arms froze mid-weld. The 50 chassis for cars moving down the line were ruined. The metal was scored incorrectly, the welds were botched. All that raw steel and labor – a complete write-off. That's WIP inventory scrapped. Pure loss.



1%
Other

Other

The costs that fall under this category may differ. A more significant risk is regulatory compliance. OT environments are often governed by strict standards such as IEC 62443, NIS2, or GB/T. Non-compliance can result in substantial fines, legal liability, or forced operational shutdowns.

Discover Kaspersky's comprehensive approach to OT cybersecurity

The goal of spending money on cybersecurity before an attack is to make this entire «disaster bill» as small as possible.

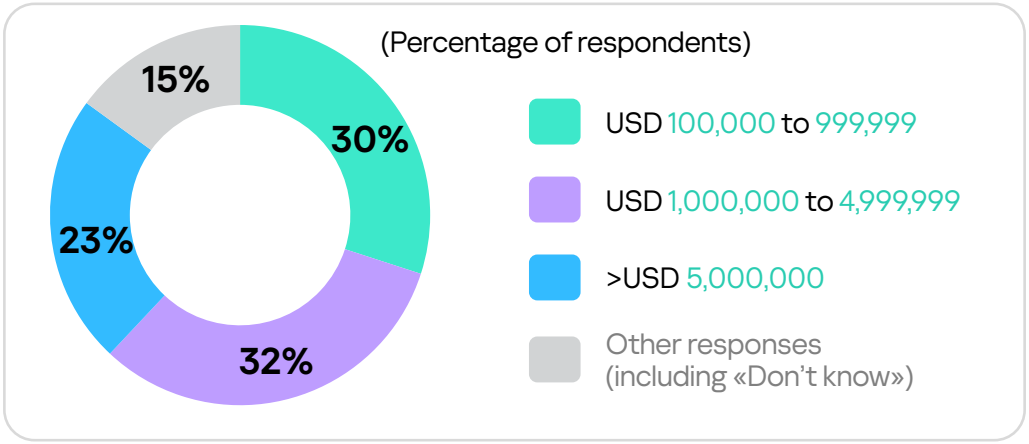
3. Comparing the results on the total estimated financial losses with your peers

To understand the total financial impact of a breach, you must consider not only breach-related costs (such as those for incident response payments and production recovery investments), but also those associated with lost revenue opportunities or lost production time, as shown in the exhibit above. Accounting for each aforementioned cost category, nearly a quarter of our survey respondents estimated cyberattack-related financial damages of more than USD5,000,000 per incident across 2023 and 2024.

These costs can vary by region, industry and other organizational factors. For service-oriented OT organizations, outages can also lead to significant reputational damage and legal liabilities from broken contracts – costs that are harder to quantify but often more severe.

According to VDC Research, respondents reported the costs of cybersecurity breaches as follows:

Estimated cost of financial losses to an organization caused by cybersecurity attack(s) or breach(es)



4. Mapping the cybersecurity spending to business objectives

Align your security issues with the overall risk framework. Select one, two or several relevant areas and tie OT cybersecurity spending to management core goals, for example:

Risk transfer: Improving insurance coverage

The question of insurance coverage in the event of a lawsuit is critical. The insurance is not a guarantee of payment; rather, it's contingent on demonstrating due diligence. If an incident occurs and you lack basic protections, your claim could be denied. The organization must not only understand the cost of this insurance but also, more importantly, ensure their risk mitigation practices meet the required standards to keep that coverage valid.

Reputation: Maintaining trust as a reliable partner

Beyond direct financial loss, consider strategic risks that are difficult to quantify in monetary terms but pose a severe threat to the company's long-term viability:

- **Catastrophic safety failures**: In OT environments, a breach could result in physical harm, environmental disasters or loss of human life.
- **Reputational damage**: A serious incident erodes customer confidence, directly leading to increased churn and difficulty acquiring new business.
- **Compromise of client data**: The leakage of sensitive client information exposes the organization to regulatory penalties and legal action.
- **Cascading operational impact**: Failures within ICS systems can ripple outwards, halting your clients' processes and resulting in substantial contractual repercussions.
- **Erosion of competitive position**: The cumulative effect of these risks is a loss of market share.

Operational efficiency: Investing in resilience

Every dollar spent is not about stopping hackers; it's about ensuring that production lines run without interruption, shipments go out on time and the balance sheet is protected from catastrophic loss.

What does your CFO want to see?

- **Reduced costs and risks.**
- **Increased productivity and growth of revenue.**

For the security challenge, you must recommend a solution and demonstrate how it fits within this framework. Clearly articulate the risk you are solving and the security issue you are mitigating. Simply put, you must communicate how the security issue impacts the business.

Explain how the problem affects the way the organization operates. This business impact is far more important to executives than the technical details of the security risk itself.

5. Analyzing an offer for the required cybersecurity solutions and measures

such as industrial-grade endpoint protection and infrastructure visibility solutions; threat detection, prevention and response solutions; and appropriate managed services.

Develop a comprehensive investment plan that accounts for the total cost of ownership, including not only initial and annual fees but also expenses for migration, planning, consulting and training.

If an industrial organization lacks proper software to protect its workstations from cyberattacks and uses IT-grade endpoint security agents, it may pose risks to production continuity. The traditional endpoint security solution could clash with legitimate industrial control systems, causing downtime, or it may lack OT-specific threat protection functions. Both scenarios may negatively affect production. As an industrial-grade solution, Kaspersky Industrial CyberSecurity (KICS) helps you attain visibility into your OT environment, get awareness of vulnerabilities and applicable risks, discover configuration changes or anomalies, and protect your industrial hardware and software components from threats. Through optimized OT-specific product functions that have no impact on production operations, KICS helps to minimize the risk of cyberattacks and prevent downtime. Kaspersky services may augment protection with threat intelligence, security assessment, incident response and more.

Kaspersky
OT CyberSecurity

Request your customized offer

www.kaspersky.com

Explore the threat landscape for industrial automation systems at ics-cert.kaspersky.com.

© 2025 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

#kaspersky
#truetobusiness