DRAGOS

REPORT

2025 OT Security Financial Risk Report

Assessing Operational Technology (OT) Security Efficacy with Independent Insurance Industry Analysis by Marsh McLennan

Table of Contents

Executive Summary 04

Key Data Points 05

Key Takeaways 06

Top Three Challenges of Managing and Insuring OT Cyber Risk 07

Forecasting Financial Risks from Global OT Cybersecurity Breaches 09

How the Data is Derived 10

What's At Risk 10

Average at Risk Within BI Claims 11

Likelihood of Impact 13

Strategic Insights for Risk Managers and Insurance Stakeholders 16

SANS ICS 5 Critical Controls 17

Risk Reduction Findings 18

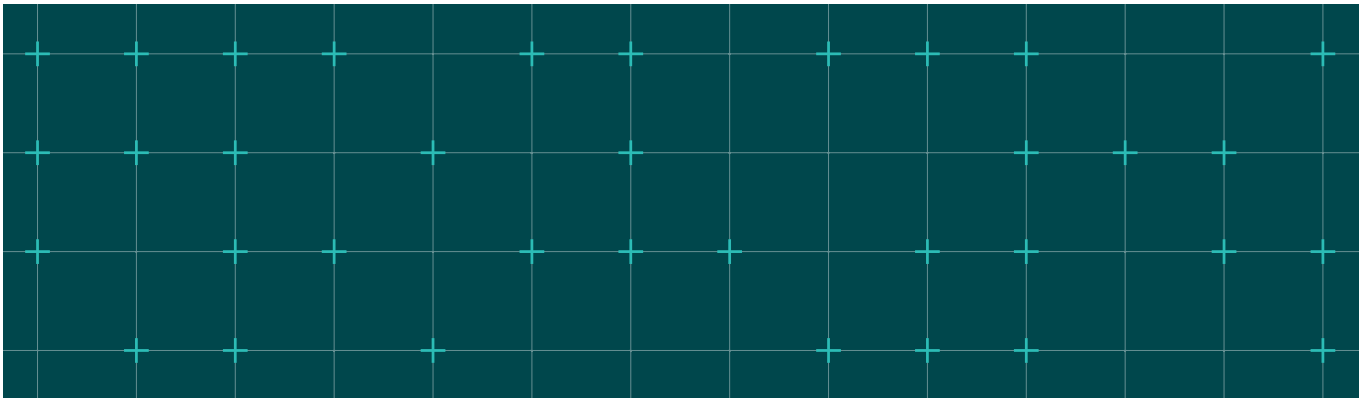
Findings Impacts 20

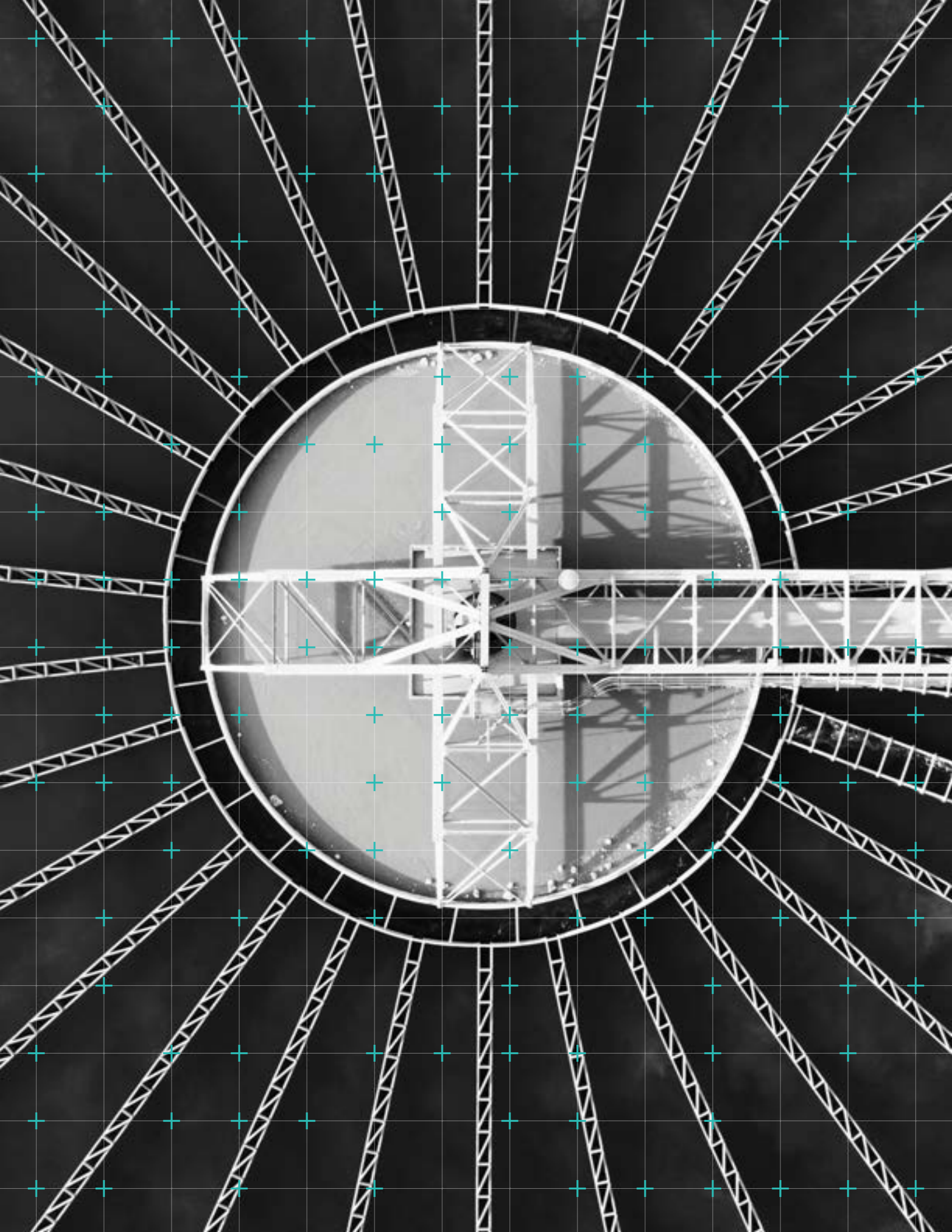
What the Findings Mean for Stakeholders: Dragos Recommendations 21

Dragos-Recommended Next Steps 23

Steps and Considerations for Specific Stakeholders 24

Appendix & Methodology 25





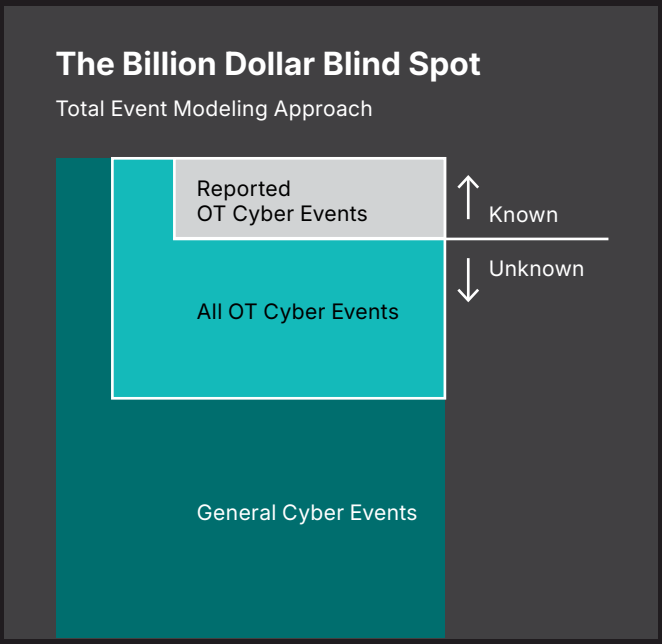
Executive Summary

This study is a groundbreaking investigation into the financial impact of cyber incidents involving operational technology (OT) assets and provides important estimation of potential future OT cyber breach losses, as analyzed by insurance statisticians.

More critically, the study applies statistical modeling to identify and quantify the most influential OT cyber risk controls and their potential risk reduction impact.

The statistical analysis referenced in this report is based on data compiled and modeled by the Marsh McLennan Cyber Risk Intelligence Center (CRIC), Marsh McLennan's enterprise-wide global cyber data, analytics, and modeling center of excellence.

The proprietary data and models used are based on the past 10 years of information security events and claims, drawn from some of the largest insurance claims databases in the world.



What It Covers

The first part of the report focuses on estimating the financial risks associated with worldwide cybersecurity breaches involving OT assets. The second part of the report statistically models how various controls can potentially reduce the likelihood and severity of financial loss.

Who It Is For

01.
Critical Industry Risk Executives

02.
OT Operators

03.
Reinsurers, Underwriters & Brokers

04.
Insurance Advisory & Security Consultants

Key Data Points

The following data is based on global estimates drawn from statistical modeling of the Marsh McLennan Cyber Risk Intelligence Center. For more on how the data is derived, with methodology scope and exclusions, see page 10. Based on a 1:250 tail scenario (0.4% likelihood of occurring next year):

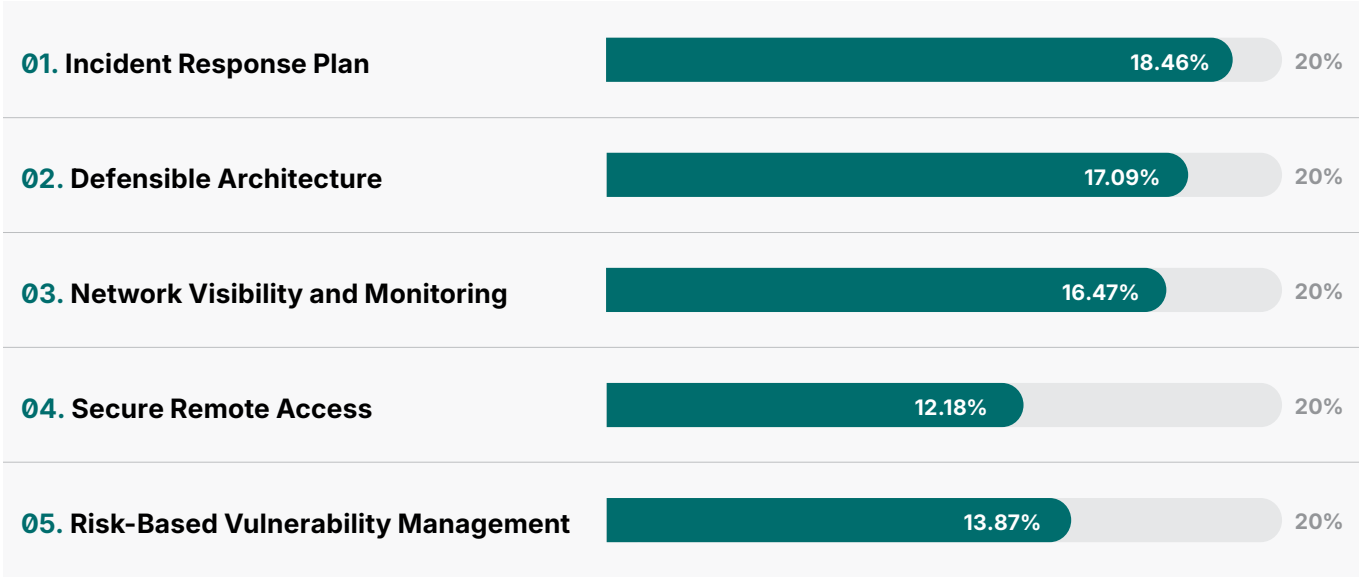
$US 329.5B

is at risk for OT cybersecurity

$US 172.4B

is at risk when BI is involved in a cyber-physical event

Using historical BI claims data with OT and cyber elements, the study modeled how cybersecurity controls reduce the likelihood and severity of financial loss. Data was mapped to the SANS ICS 5 Critical Controls framework to establish risk reduction benchmarks, with the following quantified results:



Key Takeaways

01 **Billions at Risk**

OT cyber risk is growing and expected to impact the global economy in the hundreds of billions of dollars annually.

02 **Indirect Costs Add Up**

Much of this risk comes from indirect effects to OT networks and operations, either by affecting supporting systems or through abundance-of-caution shutdowns. The complexities of interconnected OT systems can often introduce compounding aggregate risk in these environments.

03 **Regional and Industry Considerations**

Region, industry, and revenue are all important variables for determining risk levels. For example, North America and Europe have the highest OT event rates and manufacturing is the OT sector with the highest likelihood of impact. From the analysis, it is evident that revenue, industry, and region have influence and should be considered when assessing variation in cyber risk.

04 **If You Do One Thing: Prepare for Incident Response**

Incident Response Planning was the category of critical industrial control systems (ICS) cybersecurity controls with the highest correlation to risk reduction. Incident Response planning when done correctly is inclusive of defining real risk scenarios based on OT-specific threats, practicing the plan in a tabletop exercise, and testing the plan to ensure that data collection is appropriate ahead of the incident to be able to answer the questions that organizations will have in response and recovery.

Dragos has observed that executive staff and board of directors mistakenly assume that reporting and advancements in enterprise IT security are inclusive of OT environments. More often, there is significant lack of security controls and data collection inside of OT environments. This study validates that response readiness measures like planning, OT monitoring, and telemetry have significant risk reduction.

05 **Defense Is Doable**

An Incident Response Plan, Defensible Architecture, and Network Visibility and Monitoring are the top categories of cybersecurity controls with correlation to reduction in risk — but all five critical controls were shown to have significant correlation with risk reduction.

Top Three Challenges of Managing and Insuring OT Cyber Risk

The operational technology (OT) threat landscape has undergone significant transformation in the past decade as critical infrastructure has become firmly enmeshed with IT infrastructure, increasingly internet-facing, and remotely accessible. Cyber criminals, hacktivists, and government adversaries are all applying advanced techniques against OT assets to orchestrate cyber attacks and other disruptive activities that can disrupt or damage industrial operations.

In parallel, there is a concerning emergence of various groups that are either in the process of developing or have already deployed ICS-specific malware, exemplified by notable threats such as PIPEDREAM. These malware variants are specifically designed to exploit ICS environments, showcasing a targeted approach towards compromising operational technology networks.

The attack frequency keeps escalating. But until this report, OT operators, risk executives, insurance stakeholders, and regulatory bodies have all struggled to quantify the cyber risk associated with OT environments. Three major challenges are hindering effective OT cyber risk management and insurance.

→ **Challenge 1: Financial Impact of OT Risks Were Previously Undefined**

Until now, it has been difficult to quantify the potential financial impact of OT cyber risks — including what's truly at stake and the likelihood of an incident.

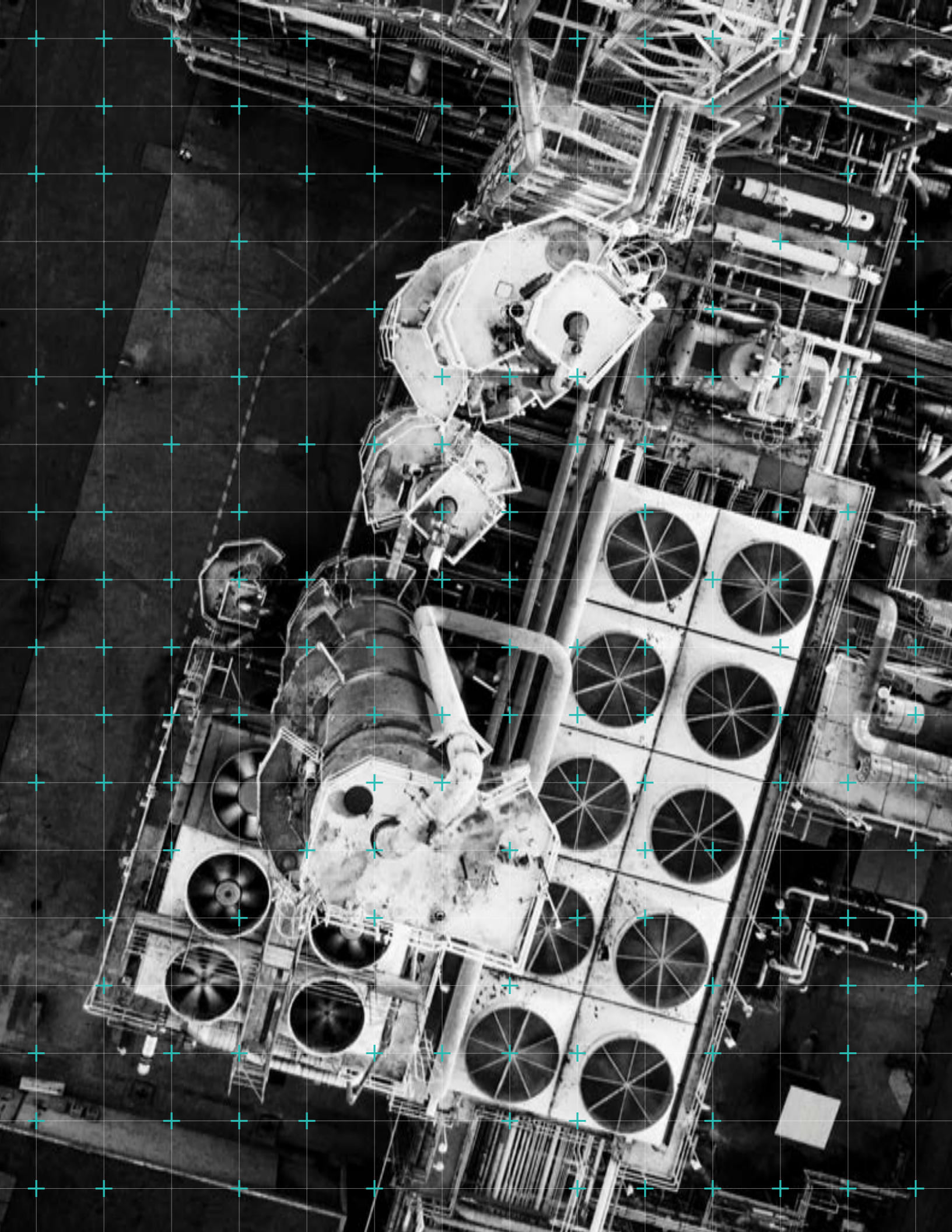
→ **Challenge 2: OT Security ROI Is Hard to Calculate**

Without clear financial impact estimates, justifying OT security investments becomes a major hurdle. Leaders can't easily quantify how cyber spend translates into meaningful risk reduction.

→ **Challenge 3: OT Operators Struggle to Prioritize Controls Improvements**

The absence of ROI insights makes it difficult for OT operators to prioritize cybersecurity controls. There has been no independent data on controls effectiveness to guide these decisions — until now.

The findings in this report equip OT risk managers with data-driven estimates to more effectively address these challenges and drive informed prioritization.



01.

Forecasting Financial Risks from Global OT Cybersecurity Breaches

How the Data is Derived

The data and statistical analysis referenced within this report comes from insurance industry sources completely independent of Dragos.

The financial estimates are based on Marsh McLennan Cyber Risk Intelligence Center's proprietary mix of insurance industry data from the past decade, collected and analyzed with a combination of models. The team then analyzed cyber incident claims and controls information to estimate the potential risk reduction driven by various OT cybersecurity controls.

What's At Risk

The first part of the study estimates the financial risks associated with worldwide cybersecurity breaches involving OT assets. The analysis quantifies what's at risk and assesses likelihood of impact based on industry and company revenue.

DATA AND ANALYSIS SOURCING HIGHLIGHTS

- Data collection and analysis completed by independent insurance industry statisticians at the Marsh McLennan Cyber Risk Intelligence Center
- Data from one of the largest insurance claims databases in the world, independent third-party data, insurability reports, and breach recovery reports
- Historical OT breach reference data from 2014–2024
- Data based on confirmed incidents — consequences could be higher than modeled due to underreporting and other discrepancies
- Loss estimations based on the model with over 10,000 iterations
- This model was built to estimate insurable losses resulting from cyber events affecting OT networks, impacting commercial and public organizations. It does not include damages resulting from warfare, espionage, or pre-positioning. Additionally, it does not include effects to individuals.

Average at Risk Within BI Claim

The first calculation estimates OT cybersecurity financial risks that will involve BI in a typical year. This is based on historical claims information involving OT disruption or extortion.

Estimate: $US 12.7B as the average in total annual risk where BI claims are made.

Average Financial Risk

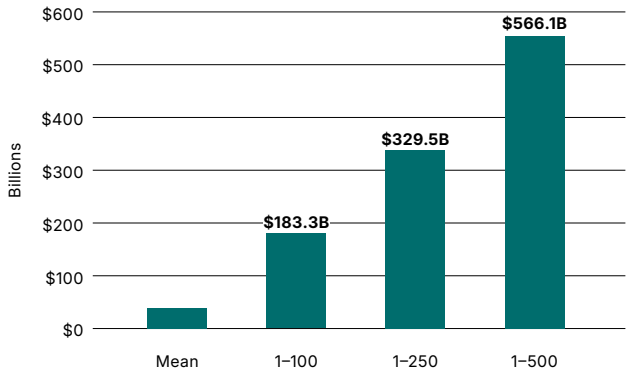
This second calculation is an estimation of the average total financial risk expected from OT cybersecurity incidents over the next year. This is based on incident information regardless of whether a BI claim was filed.

Estimate: Up to $US 31.1B as the average globally aggregated OT-related cyber risk over the next 12 months.

Tail-Model Scenario Risk

The analysis also examined the risk for edge cases. These are scenarios that may involve major supply chain ripples or other extraordinary events. The edge cases increase quickly in the model. The following is based on a 1:250-chance tail model (i.e., a 0.4% likelihood).

Global Insurable Losses



Estimate: Worst-case OT cyber incidents that result in a BI claim could trigger $US 172.4B in a single year. Averaged across all industries globally, $US 329.5B could be at total risk for OT cybersecurity in a single year.

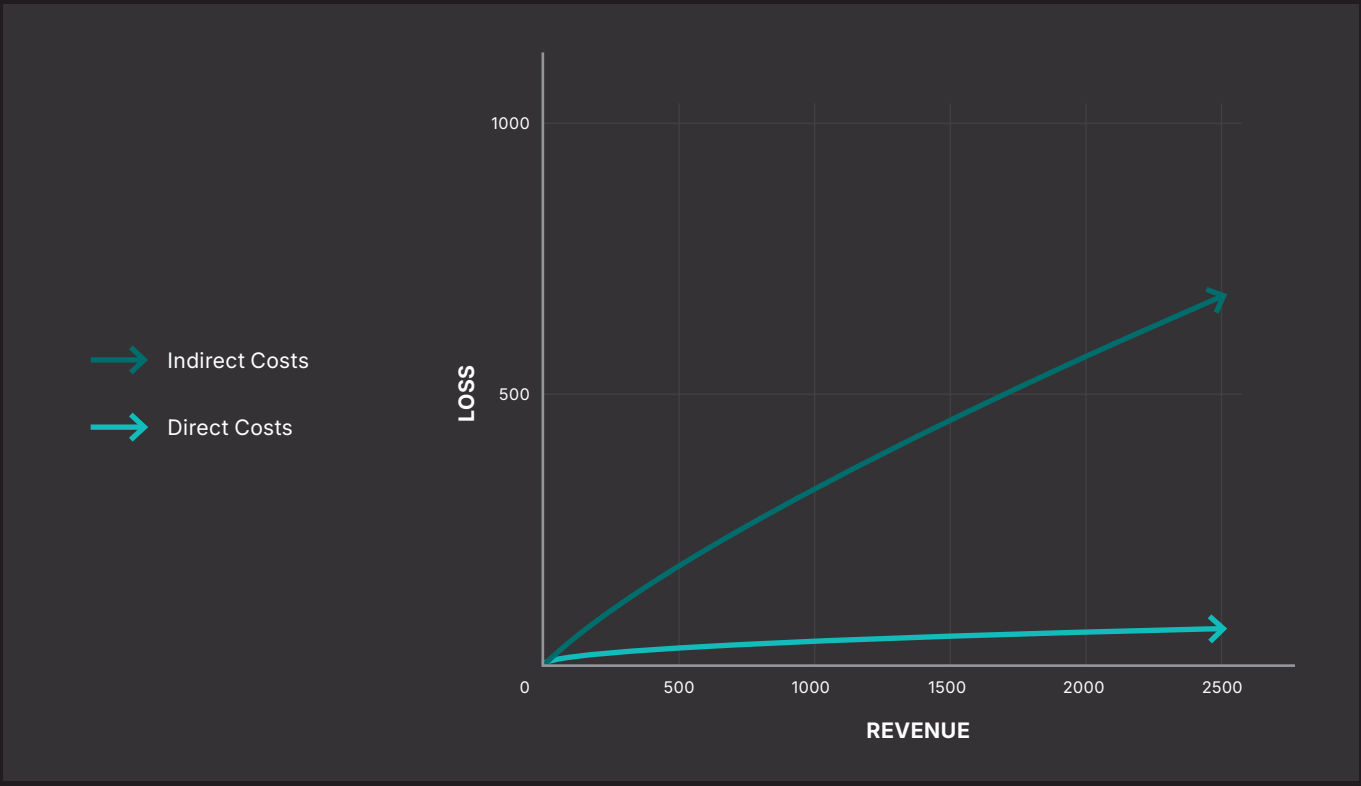
Indirect vs Direct Costs

Much of the financial risk forecasted in the above figures come from indirect effects to OT networks and operations. These costly impacts could ripple across OT-dependent businesses, considering equipment compromise or damage versus follow-on effects to supporting systems or abundance-of-caution shutdowns.

The model estimates that not only are indirect costs more likely—impacting roughly 70% of the breaches that affect OT—but they also incur a steeper cost curve over time. While direct breach costs are typically bound by predictable remediation costs, indirect costs tend to be 'blank check' losses incurred due to business interruption and long-term fallout.

The analysis found direct versus indirect cost curves change relationship based on revenue. As revenue increases, indirect costs tend to outpace direct loss. Organizations can, and often do, experience indirect loss without experiencing a direct loss. Importantly, this emphasizes the importance of considering total risk and business resiliency versus OT damage while stressing the importance of visibility, operational resilience, and incident response planning over focusing only on prevention.

MODEL: Indirect vs Direct Costs



Likelihood of Impact

Likelihood Findings

The likelihood that a breach would occur in a given industry was assessed by querying the historical breach data on percentage of occurrences and extrapolating an expected future range based on regression modeling. The total number of expected breaches based on historical data, the total number of companies in the sector/region/revenue band, varying threat levels between revenue bands ($US 10B generally encounters more threats than $US 1M), as well as attributes like expected visibility in that region (for example, it is possible the breach rate is underreported in regions without maturing regulation or security tooling) were taken into account.

With some exceptions, increased revenue generally correlates with an increased likelihood, across industries and sectors. Additionally, regional variations impact likelihood by sector.

General Likelihood		Regional Likelihood				
Sector	General Likelihood	APAC	EU	IMEA	LATAM	NA
Construction	0.27%	0.11%	0.11%	0.48%	0.07%	0.60%
Manufacturing	0.71%	0.32%	0.49%	0.35%	0.19%	1.64%
Building Automation & Warehousing	0.37%	0.22%	0.25%	0.14%	0.09%	0.87%
Utilities	0.26%	0.08%	0.10%	0.90%	0.48%	1.14%
Healthcare/Hospitality	0.23%	0.02%	0.05%	0.01%	0.01%	0.14%
Oil and Gas	0.45%	0.39%	0.19%	0.65%	0.32%	0.66%
Manufacturing Subgroups						
Chemical Manufacturing	1.49%	0.66%	1.02%	0.74%	0.40%	3.43%
Food and Beverage	1.25%	0.55%	0.85%	0.62%	0.33%	2.87%
Pharma	1.43%	0.63%	0.97%	0.71%	0.38%	3.28%
Utility Subgroups						
Electric Power Generation, Transmission and Distribution	0.49%	0.16%	0.19%	1.72%	0.92%	2.17%
Natural Gas Distribution	0.05%	0.02%	0.02%	0.17%	0.09%	0.21%
Water, Sewage and Other Systems	0.24%	0.08%	0.09%	0.82%	0.44%	1.03%
Other Subgroups						
Oil and Gas Extraction	0.39%	0.33%	0.16%	0.55%	0.27%	0.56%

Looking over the previous 10 years, the historical percentage of total OT-related breaches, averaged by year, were the following.

- **Manufacturing: 15.59%**
- **Utilities: 2.45%**
- **Building Automation: 2.62%**
- **Construction: 26.92%**
- **Health Care: 27.4%**

This serves as a starting point for likelihood, but as described above, multiple other factors are then combined to arrive at likelihood for a given organization.

Industry Findings

All sectors face increasing OT cyber risk. While the rise isn't always year-over-year, the overall likelihood has grown steadily over the past decade. This trend is shaped by multiple factors — including policy and coverage changes, evolving regulations, global events, and shifting attacker incentives.

02.

Strategic Insights for Risk Managers and Insurance Stakeholders

SANS ICS
5 Critical Controls:

01. Incident Response Plan

02. Defensible Architecture

03. ICS Network Visibility & Monitoring

04. Secure Remote Access

05. Risk-Based Vulnerability Management

Risk Reduction Findings

The second part of the study offers the greatest insight for risk managers and insurance industry stakeholders. Marsh McLennan used proprietary data to analyze historical metrics through the lens of risk reduction.

Using available historical data from BI claims with OT and cyber components (including insurability questions and information collected during claims), the study modeled how various controls reduce the likelihood and severity of financial loss.

By mapping data against the SANS Institute's 5 Critical Controls for ICS Cybersecurity, benchmarks were established for estimated risk reduction. The SANS cybersecurity controls were chosen because they stand as the leading framework for building a cyber-resilient OT infrastructure.

The potential risk reduction impact was then quantified for each control. For example, risk-based vulnerability management showed greater estimated impact than secure remote access. Incident response planning stood out as the most impactful control, according to the insurance experts.

SANS ICS Critical Control	Average Risk Reduction
Incident Response Plan	18.46%
Defensible Architecture	17.09%
Network Visibility and Monitoring	16.47%
Secure Remote Access	12.18%
Risk Based Vulnerability Management	13.87%

The weighting measures for risk reduction in the table above provide an unprecedented data-driven approach to prioritizing OT cybersecurity investment. For example, the percentages in the next table show that even for organizations with limited resources, it makes sense to prioritize incident response planning and readiness first before addressing secure remote access.

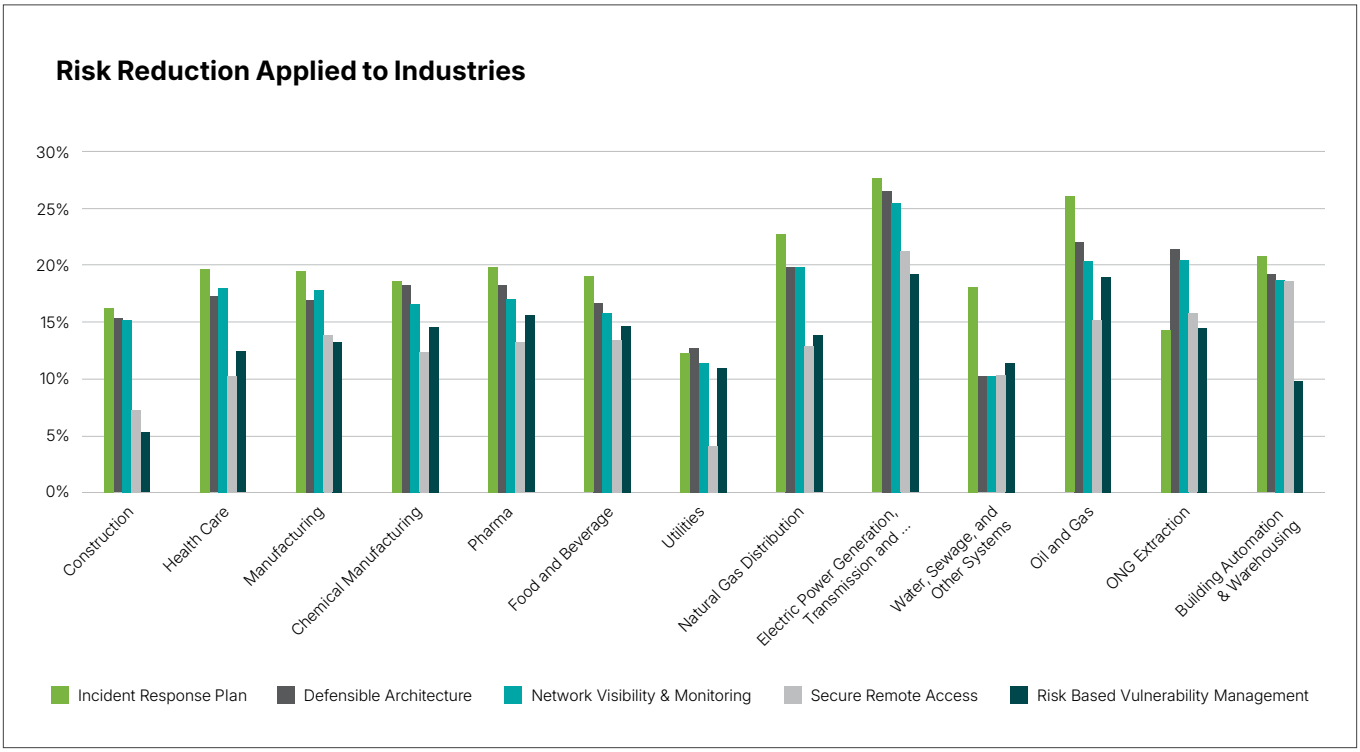
The percentages and those on predicted financial losses provide numerical proof that targeted investments in critical controls across global OT assets could help critical industries avoid billions in potential losses.

It's important to note that that these controls are not purely additive—implementing all five controls wouldn't necessarily result in a 78% risk reduction. Some controls are interrelated, making it difficult to accurately predict the combined impact with current data. However, the individual percentages remain valuable, as they confirm that each control delivers measurable risk reduction.

Risk reduction through security controls can be estimated with tangible financial returns. Tying each control to an estimated dollar value is also contingent on organizational variables that include industry and revenue, as well as other difficult to quantify factors like maturity of controls deployment.

Organizations must recognize that deploying, implementing, and operationalizing cybersecurity controls is an ongoing process — not a one-time effort. The quality of deployment and the effectiveness in how controls are operationalized are critical factors not modeled here and remain difficult to quantify. Still, the reality is clear: continued investment is essential to sustain and maximize risk reduction over time.

	SANS ICS 5 Critical Controls				
Sector	**Incident Response Plan**	**Defensible Architecture**	**ICS Network Visibility & Monitoring**	**Secure Remote Access**	**Risk-Based Vulnerability Management**
Construction	**16.25%**	**15.33%**	**15.19%**	**7.32%**	**5.31%**
Healthcare	**19.63%**	**17.20%**	**17.89%**	**10.27%**	**12.40%**
Manufacturing	**19.38%**	**16.87%**	**17.70%**	**13.78%**	**13.22%**
Chemical Manufacturing	**18.61%**	**18.24%**	**16.56%**	**12.24%**	**14.49%**
Pharma	**19.73%**	**18.17%**	**17.02%**	**13.19%**	**15.50%**
Food and Beverage	**18.97%**	**16.67%**	**15.82%**	**13.37%**	**14.63%**
Utilities	**12.19%**	**12.62%**	**11.39%**	**4.08%**	**10.91%**
Natural Gas Distribution	**22.65%**	**19.75%**	**19.75%**	**12.83%**	**13.72%**
Electric Power Generation, Transmission, and Distribution	**27.58%**	**26.45%**	**25.42%**	**21.13%**	**19.11%**
Water, Sewage, and Other Systems	**17.98%**	**10.11%**	**10.11%**	**10.22%**	**11.31%**
Oil and Gas	**25.99%**	**21.99%**	**20.31%**	**15.12%**	**18.90%**
Oil and Gas Extraction	**14.24%**	**21.32%**	**20.44%**	**15.71%**	**14.38%**
Building Automation and Warehousing	**20.70%**	**19.14%**	**18.66%**	**18.55%**	**9.81%**



Findings Impacts

Estimating the potential financial losses expected from OT cyber breaches and the risk reduction probability of the top five critical cybersecurity controls provides groundbreaking data to OT operators and risk executives, and even insurance industry stakeholders.

The fact remains that OT cybersecurity does not have the historical metrics other insured industries have. Insurability questions, forms, categorization of events, and information collected during a claim are evolving and the insurance industry is still standardizing methods for estimating OT cyber financial risk and the factors that can help companies avoid losses.

Additionally, other unique nuances remain to be navigated — for example, OT often straddles ground between cyber and physical coverage policies. Cybersecurity claims often don't identify whether an incident was IT or OT, and some incidents are claimed under physical policies.

Nevertheless, the sophisticated analysis conducted for this study helps fill statistical gaps as these standards emerge. The findings lay statistical foundations for quantifying OT cyber financial risks and risk reduction from common controls.

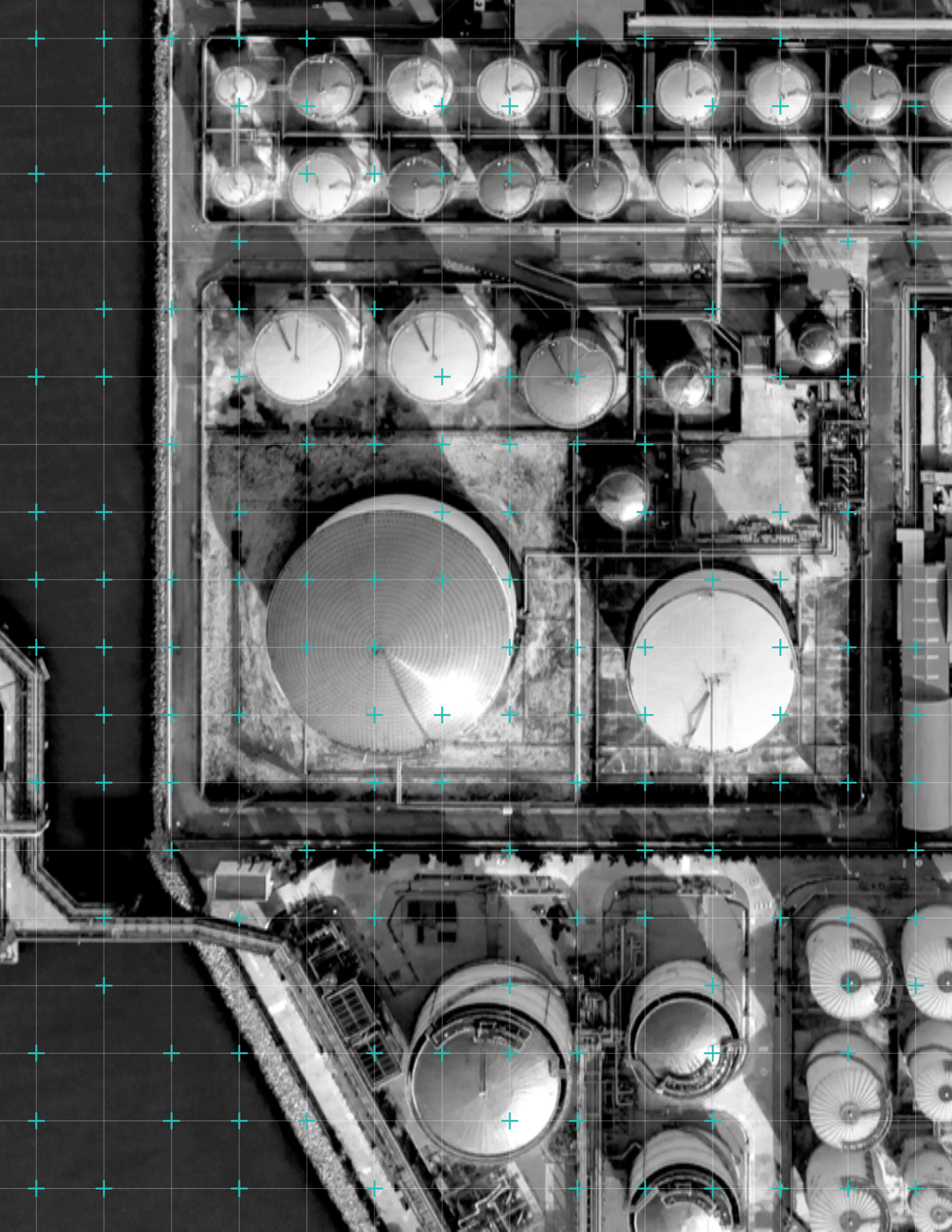
What the Findings Mean for Stakeholders: Dragos Recommendations

01 **OT security ROI considerations:** The metrics in the study provide one of the first instances of an estimated financial return on investment that the industry has thus far. While not a direct ROI calculation, it helps to estimate avoided losses, which can offer directional guidance in the absence of better metrics.

02 **Proving value of SANS ICS 5 Critical Controls:** The analysis conducted by CRIC provides a view into the estimated financial impact that implementation of SANS ICS 5 Critical Controls can have. Each one of the controls offer the potential for meaningful risk reduction.

03 **Prioritizing weighting of critical control impact to risk reduction:** By estimating the percentage risk reduction for each of the critical cybersecurity controls, organizations now have an additional, statistics-based approach for planning their OT cybersecurity roadmap. For example, bolstering incident response readiness could be one of the most impactful places to start.

04 **Enhancing coverage and rate influence:** The findings contained here can also inform risk executives and insurance stakeholders with underwriting based on the status of an OT operator's implementation of various cybersecurity controls.



Dragos-Recommended Next Steps

The findings of the research offer strong financial correlation to the threat trends that security experts at Dragos have reported on for years. For example, Dragos threat research shows that ransomware attacks alone have increased against industrial organizations by 87% in the past year—and 75% of these events resulted in at least some disruption to operations.

The data in this report also offers concrete direction for OT operators, risk executives, and insurance stakeholders to start planning their way toward more impactful OT cyber risk management.

Findings support our recommended actions that organizations can take to secure their infrastructure:

- **Define an ICS incident response plan:** An ICS incident response plan aims to detect, contain, and recover from cyber incidents without disrupting industrial operations or safety. The plan must be actionable, tested, and integrated across security, engineering, and operations teams to ensure a coordinated and effective response. Effective plans are built against OT-specific threats that have targeted peer industries, and serve to establish requirements for other critical controls. A successful plan depends on clearly identifying the required questions and expected outcomes from the response efforts, and ensuring that data collection and detection activities within the OT networks are closely aligned and correlated.

- **Build a defensible architecture:** Building a defensible architecture reduces the attack surface, limits adversary movement, and ensures only authorized users and systems can interact with OT environments. This protects both business continuity and system integrity. A defensible architecture enables human defenders to counter threats within their environment and is tailored to the specific threats relevant to the organization, as outlined in the incident response plan.

- **Establish OT network visibility and network monitoring:** Nearly 45% of organizations assessed by Dragos over the past year lacked full visibility and monitoring of their OT networks. Detecting threats early is essential to prevent minor security issues from escalating into major operational disruptions. Achieving this requires continuous situational awareness across all assets, communications, anomalies, and threat behaviors within the OT environment. Historically, OT environments have lagged in gaining this visibility. Effective OT monitoring must happen before an incident occurs — not only to enable timely threat detection and trigger incident response, but also to ensure critical data is captured. Much of the data vital to incident response is transient and travels over the network; if it's not collected in real time, it is lost and cannot be recovered.

- **Take a risk-based approach to vulnerability management:** Risk-based vulnerability management allows organizations to focus on the vulnerabilities that matter, rather than applying patches and mitigations indiscriminately. Adversaries actively track OEM vulnerability disclosures and rapidly exploit newly exposed OT weaknesses. Security teams must prioritize vulnerabilities

that adversaries are actively exploiting or have actual impact to OT environments. Many vulnerabilities do not pose a meaningful risk to operations, and traditional industry standards like CVSS scores often have little correlation with actual risk in OT environments. In OT, it's essential to focus on compounded and aggregate risk rather than individual vulnerabilities. Implementing compensating controls is critical to maintaining security and operational integrity when patching isn't an option.

→ **Establish secure remote access:** A striking 65% of organizations Dragos assessed in the past year had insecure remote access conditions related to configurations, unpatched systems, and poor network architecture tied to remote access appliances and applications. Remote access in OT environments should be strictly controlled, thoroughly logged, and limited to only when absolutely necessary. Many organizations allow remote access for vendors, integrators, OEMs, or internal teams, increasing exposure. OT environments that were once considered isolated or segmented from IT are now increasingly connected to broader networks, including those of third parties. As a result, threats are increasingly targeting OT systems directly, without needing to pass through IT networks first—making robust remote access controls more critical than ever.

Steps and Considerations for Specific Stakeholders

This report offers industrial organizations and insurers with the analysis to start meaningful, data-driven conversations about OT security investment and prioritization. However, each stakeholder will have different next steps to consider:

- **Critical Industry Risk Executives:** Use these numbers to start data-driven, board-level discussions about OT cybersecurity budgeting and planning.
- **OT Operators:** Break down priorities into bite-sized initiatives, using risk reduction percentages as a North Star.
- **Reinsurers/Underwriters/Brokers:** The modeling in this report offers a strong foundation for negotiating insurability and policy terms based on the insured's existing OT security controls and improvements towards resiliency.
- **Insurance Advisory and Security Consultants:** These statistics help validate and show evidence of the value of controls recommended to clients.

Appendix & Methodology

The de-identified data and information feeding the analysis originates from a deep well of proprietary sources collected by the Marsh McLennan Cyber Risk Intelligence Center.

For this report, historical data about cyber breaches from 2014 through 2024 where OT was involved or directly related was examined. Due to relative forensic scarcity in OT reporting, a parallel analysis was also performed to investigate the financial damage from additional incidents in that timeframe that indicated the potential for OT impacts. The financial losses measured could include downtime costs, product loss, recovery costs, and other impact to the business' ability to deliver goods or services.

Using this information, a model was created and iterated over 10,000 times to establish confident forecasting. This statistical model is what governs the calculations and estimates contained in the report. This model was built to estimate insurable losses resulting from cyber events affecting OT networks, impacting commercial and public organizations. The model does not include damages resulting from warfare, espionage, or pre-positioning. Additionally, it does not include effects to individuals. The two approaches help to give a range of estimates and also inform estimates as to the likelihood of incidents in industries and regions where reporting has thus far been minimal, but OT risk exists.

The modeling was then applied to risk reduction by mapping insurability questions, forms, categorization of events and information collected from the claim against the SANS ICS 5 Critical Controls to determine how these measures could have helped companies avoid financial losses had the controls been in place.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East. Learn more about our technology, services, and threat intelligence offerings at dragos.com.

© 2025 Dragos, inc. All Rights Reserved.

DRAGOS