FORTINET

REPORT

The COO and Operational Technology Cybersecurity

A Report on Current Priorities and Challenges

Table of Contents

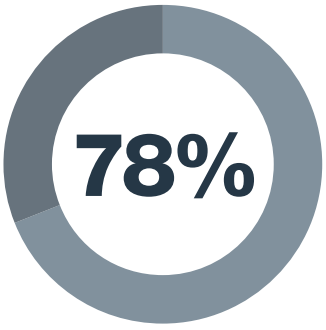
Executive Summary

The COO and Operational Technology Cybersecurity report from Fortinet examines the challenges that COOs face when it comes to securing the operational technology (OT) infrastructure and offers insights into how they are responding to these issues. Even though the responsibility for OT security is usually shared by the CISO or other executive, COOs are relevant for OT security because their teams are often responsible for managing and purchasing the equipment used on the production line, including security tools.

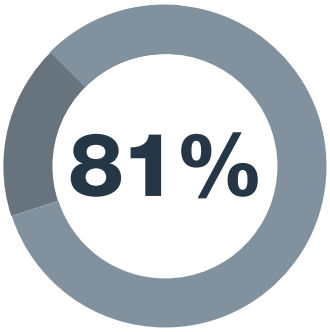
A recent Fortinet survey identified a series of insights about the COO's role in OT security. Key findings include:

1. The COO faces an **unprecedented level of change** resulting from OT/IT convergence, higher expectations of business executives, and an increasing level of involvement of the CISO in OT cybersecurity.
2. COOs worry about and struggle with **risk management challenges** far more than any other aspect of their jobs.
3. Executives are willing to approve **increases in OT cybersecurity budgets** but expect the COO to leverage these investments to deliver tangible results.
4. COOs also have difficulties **keeping pace with changes** due to the advanced threat landscape.

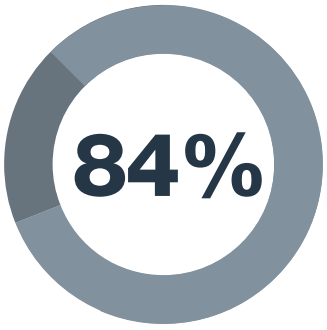
Given these trends and challenges, we analyzed the data more deeply and identified two subsets of respondents based on the number of intrusions in the previous year. We analyzed traits representative of top-tier COOs versus those of their bottom-tier counterparts to probe for explanations of the differences in security success. These best practices show that more successful COOs adroitly balance cybersecurity and operational responsibilities by tracking and reporting key cybersecurity metrics, regularly testing security and compliance, and implementing proven security measures such as multi-factor authentication.



are directly responsible for embedding security within operational processes

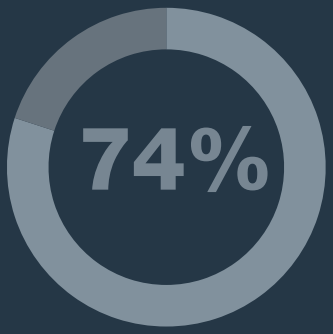


are regularly involved in the organization's cybersecurity strategy

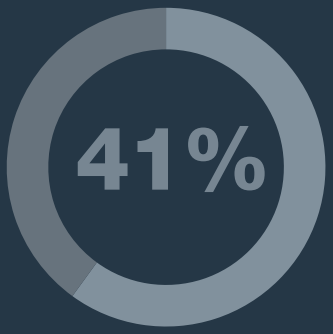


84% are regularly included in cybersecurity purchasing decisions

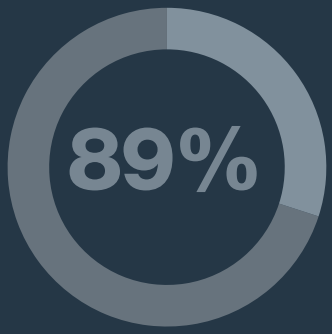
Infographic: Key Findings



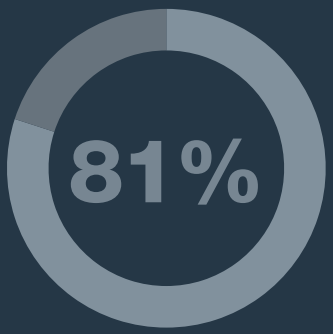
of respondents manage at least 100 devices



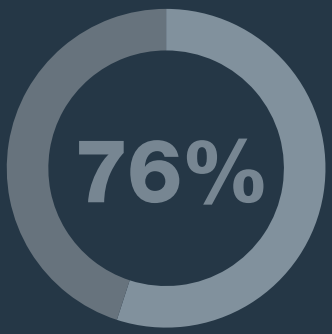
have more than 250 devices deployed



experienced intrusions in the past 12 months



experienced outages during these intrusions



expect an increase in their 2019 security budget, with 1 in 10 anticipating a ***dramatic*** increase

Top-tier COOs are:

168% more likely to cite regulatory changes as a major success challenge

124% more likely to work in organizations in which a C-level executive oversees cybersecurity

79% more likely to rank production floor efficiencies as a top success metric

45% more likely to schedule compliance reviews

Introduction

OT refers to the infrastructure that monitors and controls processes and production activities in manufacturing plants, power grids, water utilities, oil and gas extraction, transportation, and more. OT has traditionally relied on hardware and software developed specifically for industrial needs. As a result, OT and IT infrastructures have been separate entities historically, both physically and from a management standpoint.

Many OT networks are unsegmented with a mixture of production protocols, unidentified assets, and legacy devices. Some have unsecure communication channels to corporate/IT networks, while others lack connections to the internet and other external networks entirely. In general, OT is opening up to the outside world. For example, a recent survey found that 34.5% of control networks are connected to the internet and 66.4% are connected to either a third-party private infrastructure or to their enterprise business network.[1]

The industry trend is to converge OT and IT infrastructures, which benefits the organization in several ways. When OT and IT infrastructures are siloed, sharing data is a ponderous process that is only performed monthly or quarterly. By creating a common platform for OT and IT data, organizations can generate key performance indicators (KPIs) in real time based on up-to-date information from both groups. Real-time KPIs facilitate more rapid responses to changes in the marketplace, for example, by alerting product managers of a sudden increase in the cost of raw materials that affects profit margins. Managers in both groups benefit by having companywide visibility and the ability to work collaboratively across the IT/OT divide.

However, IT/OT convergence has important implications for security:

- **Expanded attack surface.** Connecting the OT and IT infrastructures exposes each to attacks from the other's endpoints. Relatively insecure OT devices such as valves, pumps, sensors, electronic locks, thermostats, and robots now are potential entry points to the IT infrastructure. In the other direction, cyberattackers can target critical utilities, such as the electrical grid and transportation systems, using the mobile network as an entry point.
- **Increased complexity.** OT network environments are complex, with anywhere from 50 to 500 devices to monitor and secure, usually from a mix of vendors. This complexity exacerbates the challenges surrounding visibility and personnel, as each device stores its own data and has specific security configuration needs and requirements.
- **Advanced threat landscape.** Connecting OT to the internet exposes the OT infrastructure to a range of legacy malware that is easily caught by signature-based IT security solutions but may still be effective on insecure industrial devices. Cyber criminals often test old malware by attacking a small number of machines, and then use the successful exploits to mount large-scale attacks. This "threat recycling" allows attackers to maximize the value of existing malware before investing in more sophisticated attacks geared to the OT world.[2]

"The expanding attack surface causes us to take more precautions to protect our database systems."

– Energy Sector Survey Respondent

"Increased complexity forces us to spend more time on cybersecurity at the expense of production operations."

– Manufacturing Sector Survey Respondent

"The advanced threat landscape is causing the team to spend many more hours each week beefing up security."

– Healthcare Sector Survey Respondent

Methodology for This Study

The COO and OT Cybersecurity report is based on a survey of COOs. Our respondents come from companies with more than 2,500 employees in a variety of industries, with more than half (59%) in manufacturing and more than a quarter (27%) from the energy and utilities sector.

Our analytical steps included the following. First, this study utilizes survey data to identify several current trends around the COO's role in securing the organization's OT infrastructure. Next, we analyze the freeform answers that respondents gave to several open-ended questions about their key challenges and construct a picture of what impacts their daily work. Finally, we delve more deeply into the data to identify a subset of organizations that experienced three or fewer intrusions over the past 12 months, and another subset that had more than four intrusions in the past year. We compare the two groups and identify best practices more likely to be practiced by "top-tier" COO leaders regarding OT cybersecurity.

OT Cybersecurity Trends for the COO

Trend: The COO is responsible for OT cybersecurity and influences the organization's security strategy.

More than three-quarters of respondents place OT cybersecurity within the COO organization, with 7 out of 10 indicating that it reports to the OT director/manager of cybersecurity and another 8% to the VP/director of network engineering/operations (Figure 1). The vast majority (81%) of COOs are regularly involved in formulating cybersecurity strategy, while the remainder are occasionally involved (Figure 2).

Given that OT and IT are still siloed in many organizations, it makes sense that the COO is responsible for the entire OT infrastructure, including security. As this report shows, the COO's role in cybersecurity is in transition. Indeed, while one might assume that cybersecurity responsibilities are shrinking for the COO, the opposite is actually the case.

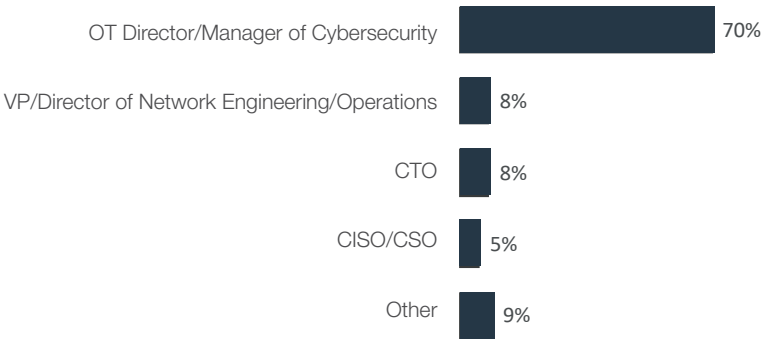


Figure 1: OT cybersecurity responsibility inside the organization.

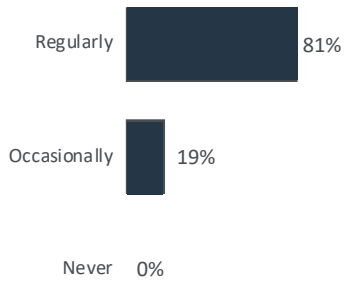


Figure 2: COO involvement in cybersecurity strategy decisions.

Trend: COO security mandate is highly visible within the organization.

It is no surprise that organizations are paying growing attention to OT security. More than half (54%) of COOs report that OT security posture is a significant factor in the organization's overall risk score, while it plays a moderate role for more than one-third (35%) (Figure 3). And risk management dominates the challenges facing COOs, a topic discussed below under "Key Challenges for the COO."

Also reflecting the heightening emphasis on security, the COO reports a wide range of metrics related to security and compliance, including results of intrusion tests (70%), security compromises (65%), scheduled security assessments (62%), and compliance with security standards and industry regulations (59% and 57%, respectively) (Figure 4).

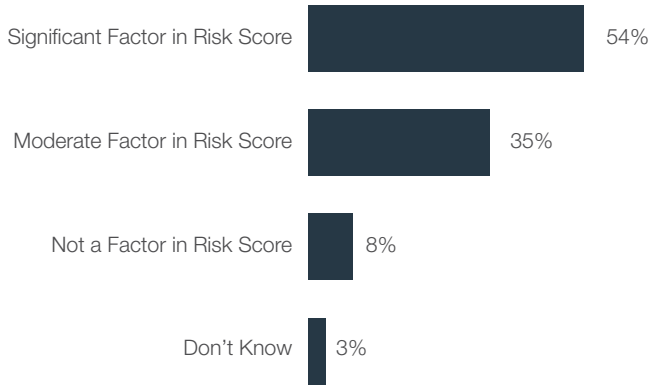


Figure 3: The impact of OT security posture on overall risk score.

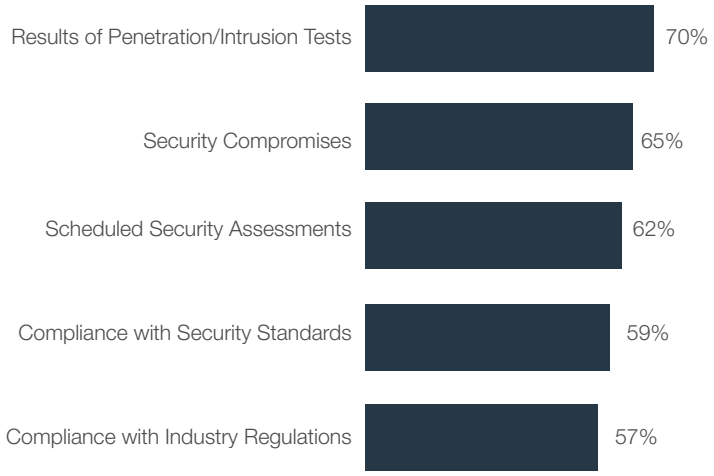


Figure 4: Reported OT cybersecurity metrics.

Trend: COOs have significant security responsibilities in addition to their traditional focus on operational factors.

The COO's primary mandate is to ensure that the organization's operations run smoothly and to keep operating costs under control. More than 8 in 10 have direct responsibility for managing production efficiency (86%), supervising operations teams (86%), selecting and managing operational tools (86%), managing quality control (81%), and supervising technicians and engineers (81%). All of these areas fall within the COO's traditional role of ensuring that the organization's operations run smoothly and keeping operating costs under control.

Beyond these tasks, organizations expect COOs to work with the CISO and other security executives to help secure the production infrastructure. More than three-quarters (78%) of respondents report that they are responsible for securing operational processes, a task for which they often have little training and experience (Figure 5). A recurring theme in this report is the need for COOs to balance increasing security responsibilities with traditional operational duties. `

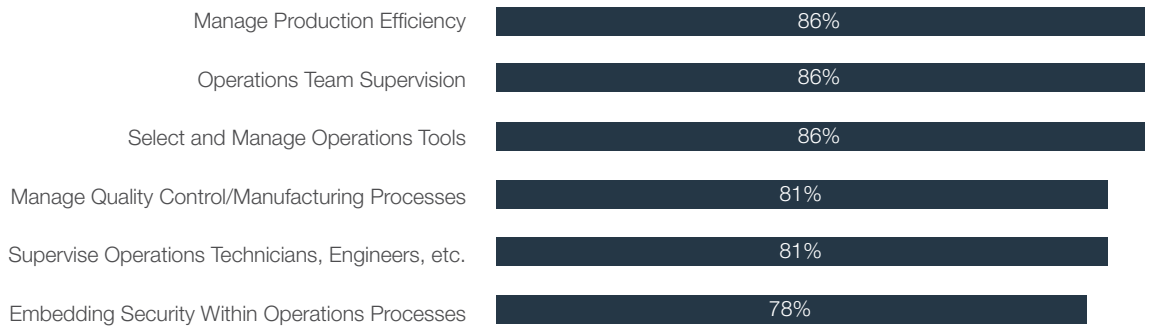


Figure 5: Direct responsibilities for COOs.

Trend: Most COOs experienced multiple intrusions in the past year, with significant damage to the business.

For the COOs in this survey, multiple intrusions are the rule, not the exception. Only 11% of COOs reported no intrusions in the previous 12 months. Of those experiencing intrusions, 42% had one or two intrusions, while the other 47% experienced three or more intrusions (Figure 6). The types of attacks varied widely, with 69% experiencing malware and more than 41% reporting spyware and phishing attacks (Figure 7).

Among the respondents with intrusions, 81% reported outages in the OT infrastructure that affected productivity (53%), put physical safety at risk (31%), or impacted revenue (28%). In contrast, the incidence of the kind of damages associated with breaches in the IT infrastructure are quite low: Slightly more than one quarter (28%) lost business-critical data and just 22% suffered brand degradation (Figure 8).

Compare these findings to a recent Fortinet study where 40% of CISOs reported outages that impacted productivity, brand value, and revenue.[3] This unfavorable comparison for OT could help to interpret other findings in this report, for example, the higher visibility of OT security and the inclusion of OT security posture in the overall risk assessment.

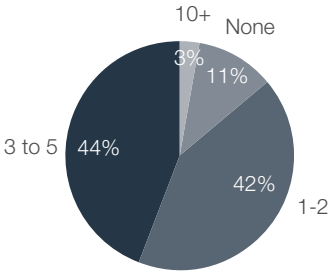


Figure 6: Number of intrusions in the past year.

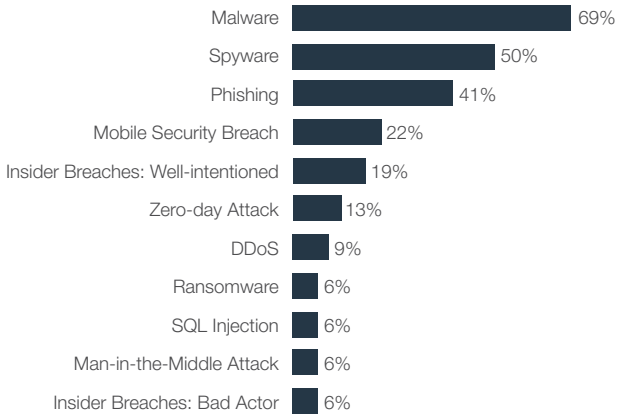


Figure 7: Types of intrusions experienced.

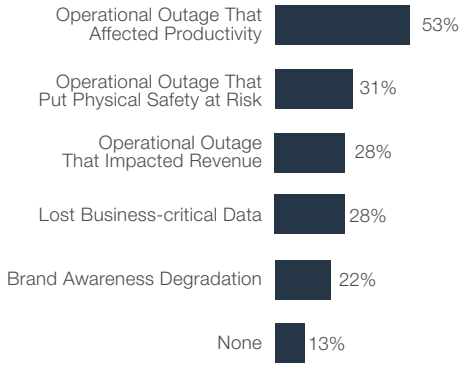


Figure 8: Impact of intrusions on the business.

Trend: Outages can negatively impact the COO's score on success metrics.

In addition to damaging the business, outages can also have a direct impact on the COO's career by making it more difficult to score well on success metrics. The top five success factors for COOs are cost efficiency (59%), productivity gains (54%), safety record (54%), production floor efficiencies (51%), and system/process uptime (30%), all of which can be negatively impacted by unplanned downtime (Figure 9).

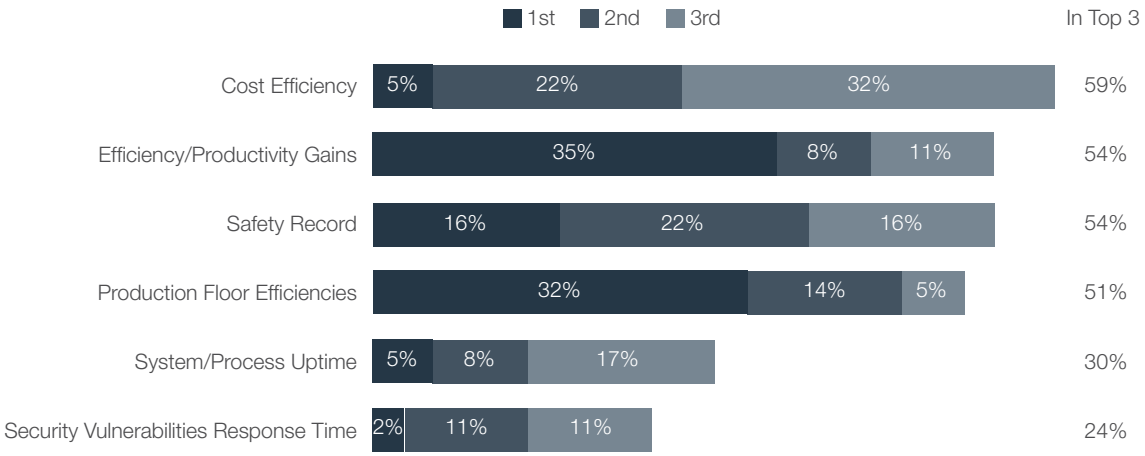


Figure 9: Success factors for COOs.

Trend: COOs expect to see their security budgets increased next year—in some cases, dramatically.

Another indication of the increasing organizational awareness of the risks of breaches in the OT infrastructure is the willingness of executives to invest in OT security. 76% of COOs saw an increase in their security budget in 2019, with 1 in 10 reporting a *dramatic* increase (Figure 10). Another survey found that OT budgets increased an average of 17.9% in 2019.[4]

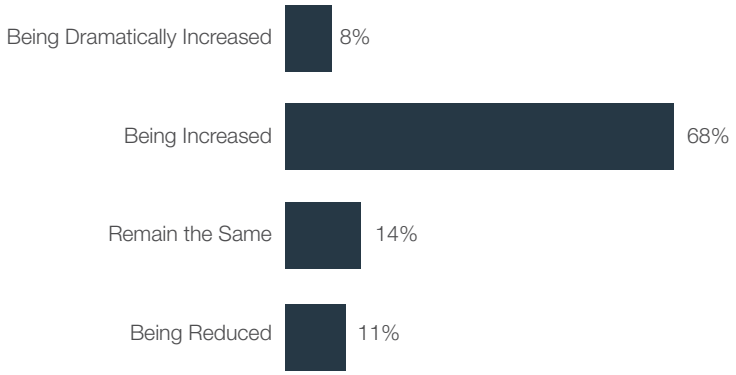


Figure 10: Trend in COO's security budgets for 2019.

Top corporate executives who authorize these investments expect the COO to deliver results in the form of fewer intrusions, higher levels of productivity, and strong compliance assessments. Reflecting these expectations, a majority of COOs track and report cybersecurity metrics for intrusions (68%), financial implications (68%), vulnerabilities found and blocked (62%), cost reduction/avoidance (57%), and tangible risk management outcomes (51%) (Figure 11). For more insights into how COOs are responding to risk, see "Key Challenges for the COO" below.

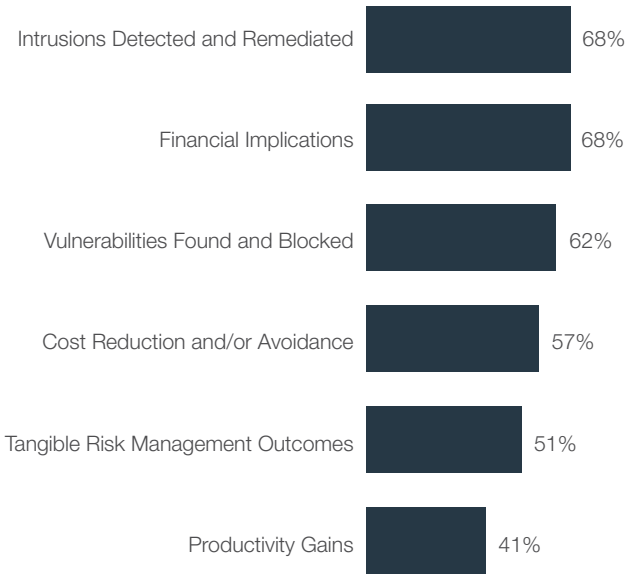


Figure 11: Cybersecurity metrics tracked and reported.

Trend: The Role of the COO is in flux as primary responsibility for OT security shifts to the CISO.

Nearly 9 in 10 (89%) respondents expect the CISO to assume primary responsibility for OT security in the next year (Figure 12). OT/IT convergence is the probable explanation, as organizations consolidate infrastructure security as a way to manage the organization's overall risk posture. Therefore, this shift should not be interpreted as diminishing the COO's cybersecurity responsibilities, which can be expected to increase as more and more cybersecurity defenses are deployed in the OT network. The expected growth in the number of smart industrial devices will also ratchet up security pressures on the COO.

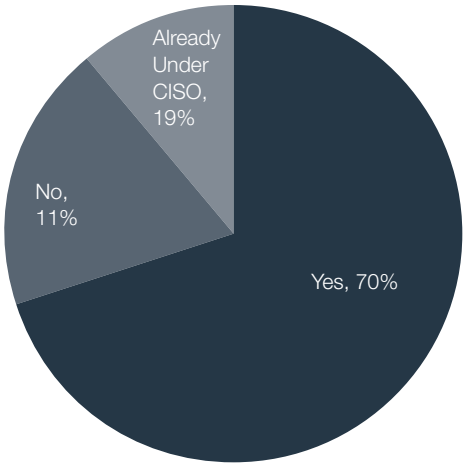


Figure 12: OT cybersecurity moving to CISO within one year.

Trend: The COO is more likely than the CISO to track and report key cybersecurity metrics.

As discussed earlier, CISOs will soon assume primary responsibility for OT security in most organizations. This trend means that CISOs and COOs will have to work together on OT cybersecurity issues, uncharted territory for both. Comparing their tendencies in measuring and reporting cybersecurity metrics reveals some interesting similarities and differences.

To begin, COOs are far more likely than CISOs to track the top four cybersecurity metrics—intrusions detected and remediated (68% versus 59%), financial implications (68% versus 46%), vulnerabilities found and blocked (62% versus 44%), and cost reduction/avoidance (57% versus 51%) (Figure 13). Though this seems counterintuitive, it makes more sense when you consider that a primary COO responsibility involves managing production processes, which are an inherently data-driven function. Thus, CISOs in OT will do well to begin using the business language their COOs employ to measure the overall efficacy of security initiatives. This approach also will enable them to more effectively communicate with other members of the C-suite, such as the CEO and CFO, as well as the board of directors.[5]

Financial implications represent the largest difference, tracked by more than two-thirds (68%) of COOs but less than half (46%) of CISOs. This finding likely reflects the importance that organizations place on profit margins, which are strongly influenced by factors under the control of the COO. Given that COOs often have more experience tracking financial implications, CISOs should take advantage of the opportunity to emulate their counterparts' best practices and put more emphasis on the financial side.

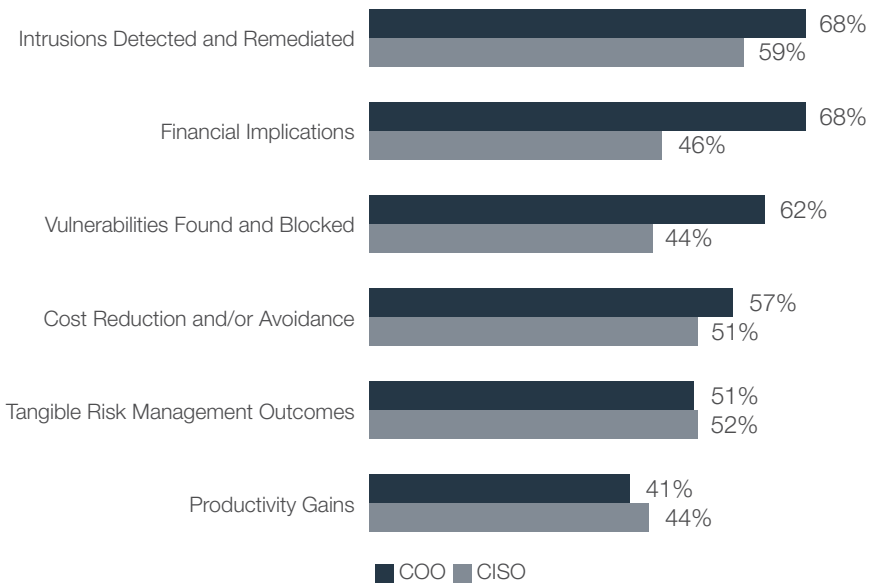


Figure 13: Comparison of metrics tracked and reported, COO versus CISO.

Trend: COOs are challenged to manage complexity as they make decisions about cybersecurity solutions.

The vast majority (84%) of COOs are regularly involved in purchasing decisions for OT cybersecurity, while the rest (16%) are occasionally involved (Figure 14). COOs report that those decisions can have negative impacts in terms of complexity (70%), adoption of security standards (54%), and operational efficiency (49%) (Figure 14). As in so many other areas, the COO must balance the need for security with the mandates of operational efficiency when making purchasing decisions. For a discussion of how complexity impacts organizational risk, see "Key Challenges for the COO" below.

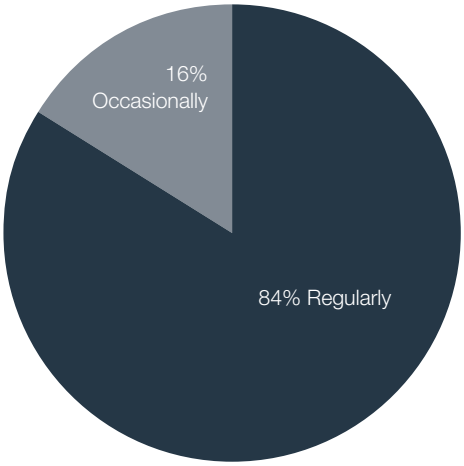


Figure 14: COO involvement in OT purchasing decisions.

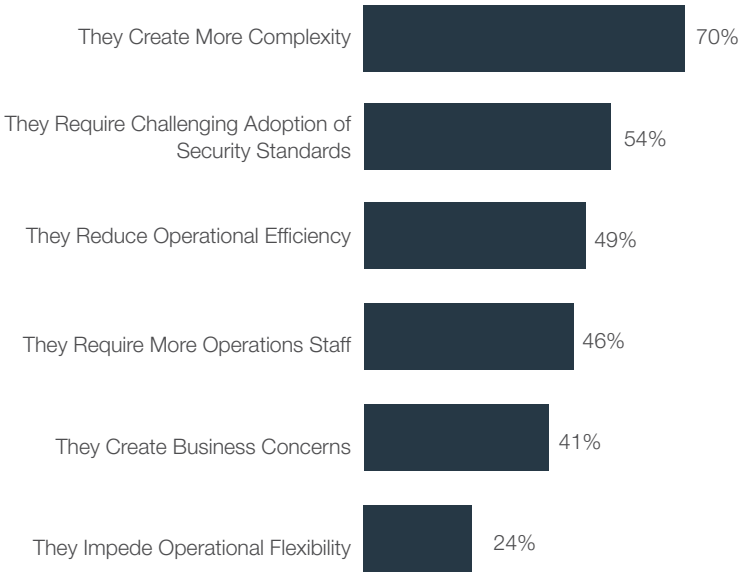


Figure 15: How cybersecurity solutions negatively impact the COO's professional success.

Key Challenges for the COO

Our survey asked respondents to answer several open-ended questions around the key challenges they face in their jobs. While responses varied greatly, we categorized their answers in order to get a feel for what is top of mind for COOs in terms of OT. The questions asked about challenges stemming from three high-level security trends: the advanced threat landscape, expanding attack surface, and increased complexity.

Challenge: A majority of COOs cite "keeping pace with change" as a major challenge associated with the advanced threat landscape.

In addition to risk management, 61% of COOs report that the advanced threat landscape makes it difficult to keep pace with change (Figure 17). This finding can be explained by the fact that many organizations are connecting the formerly isolated OT infrastructure to the outside world. As a result, OT infrastructure is suddenly bombarded by large numbers of legacy malware packages. These legacy exploits pose little threat to the IT infrastructure but can wreak havoc on certain areas of an OT system that lack signature-based protection. Thus, it comes as no surprise that COOs have trouble keeping up with this new set of challenges.

Challenge: The expanding attack surface makes it harder for COOs to manage risk, keep pace with change, and prevent intrusions.

COO respondents reveal that the expanding attack surface makes it harder for them to manage risk (65%), keep pace with change (48%), and implement defenses against attackers (26%) (Figure 18). Keeping pace with change is a recurring theme in this portion of the survey, scoring second in all three areas.

Challenge: The growing complexity of cybersecurity management is a significant contributor to the COO's workload and job stress.

OT network environments are becoming more complex just in terms of the sheer numbers of devices in operation. In this survey, 87% of respondents manage at least 100 devices, while 41% have more than 250 devices under management (Figure 16). This growth in the number of devices contributes to complexity, especially in terms of updates and maintenance.

Figure 16: Number of devices in operation.

Nearly one-third (32%) of respondents say that the complexity of managing their cybersecurity systems has increased their workload—and consequently, their stress level. Almost as many (29%) report that complexity also makes it harder to close the skills gap, which puts more pressure on the COO and undoubtedly contributes to increased workload and job stress (32%) (Figure 19).

"What keeps cybersecurity and business executives awake at night is the ever-increasing attack surface they must deal with every morning when they wake up."

– Panelist at the National Cyber Security Alliance Summit [6]

The implication of this finding is that COOs face significant challenges balancing OT cybersecurity responsibilities with mandates for availability, efficiency, and productivity. This trend is likely to intensify as the number of OT devices and complexity in managing them continues to grow.

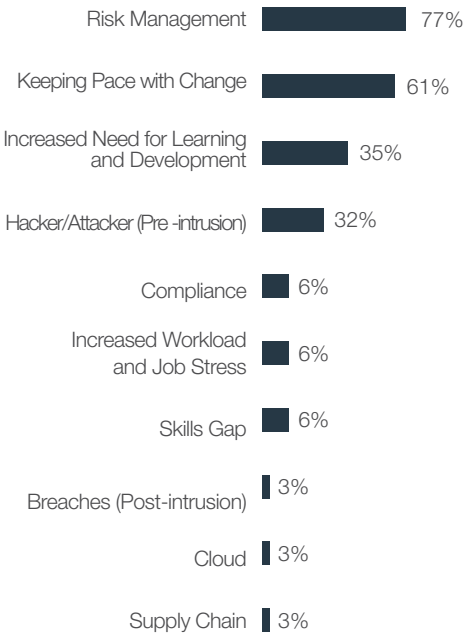


Figure 17: Challenges for COOs caused by the advanced threat landscape.

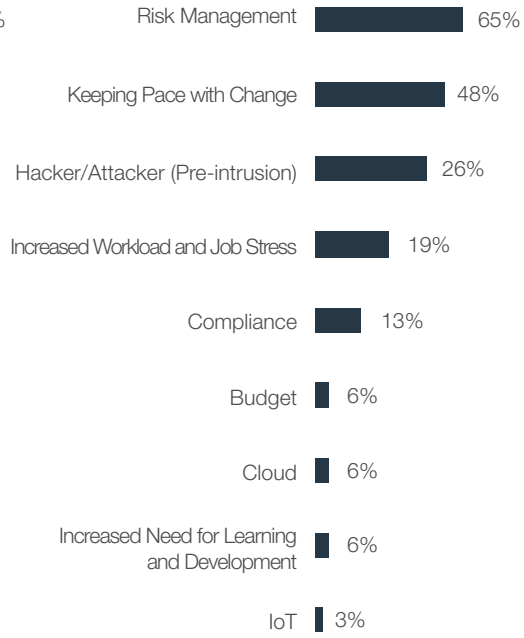


Figure 18: Challenges for COOs caused by the expanded attack surface.

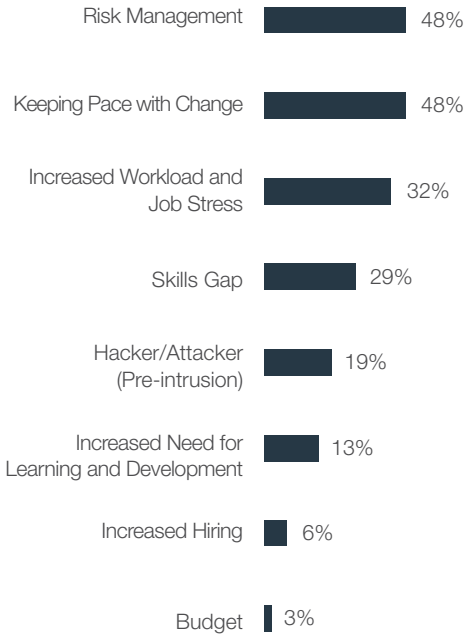


Figure 19: Challenges for COOs caused by increased complexity.

Challenge: Overall, risk management is the biggest cybersecurity challenge facing today's COO.

Cyber risk is now the top concern among businesses of all sizes. Of 1,200 business leaders who participated in a recent survey, 55% said they worry some or a great deal about cyber risks.[7]

Viewing this part of the survey as a whole, more COOs cited risk management than any other factor: 77% due to the more advanced threat landscape (Figure 17), 65% due to the expanded attack surface (Figure 18), and 48% due to increased complexity (Figure 19). This finding is consistent with the earlier finding that the OT security posture influences the organization's overall risk assessment.

To provide additional context, we compared the COO results with survey results of the CIO,[8] CISO,[9] and network engineering and operations leader[10] personas (Figure 20). Several observations stand out:

"Our institution is dealing with increased complexity by teaching our workers to manage new technology in a proactive way."

– Energy Sector Survey Respondent

- More COOs see the advancing threat landscape as posing risk management challenges than the other three personas. A positive interpretation of this finding is that COOs are well aware of the challenges posed by the relatively insecure OT infrastructure and correctly identify this reality as posing risks to the organization.
- Far more COOs and network engineering and operations leaders rate risk management as their top cybersecurity challenge compared to CIOs and CISOs. This finding does not mean that CIOs and CISOs are unconcerned about risk management, but rather reflects their priorities. For example, both CIOs and CISOs rate an increased need for learning and development as a bigger challenge than risk management.
- CIOs are the least likely to cite risk management as the top cybersecurity challenge. This finding could reflect the fact that CIOs tend to focus more on availability and reliability than security. Another possible explanation is that the CIO simply has more experience in risk management and therefore is less likely to view factors such as the expanding threat surface as a significant impediment to managing risk appropriately.

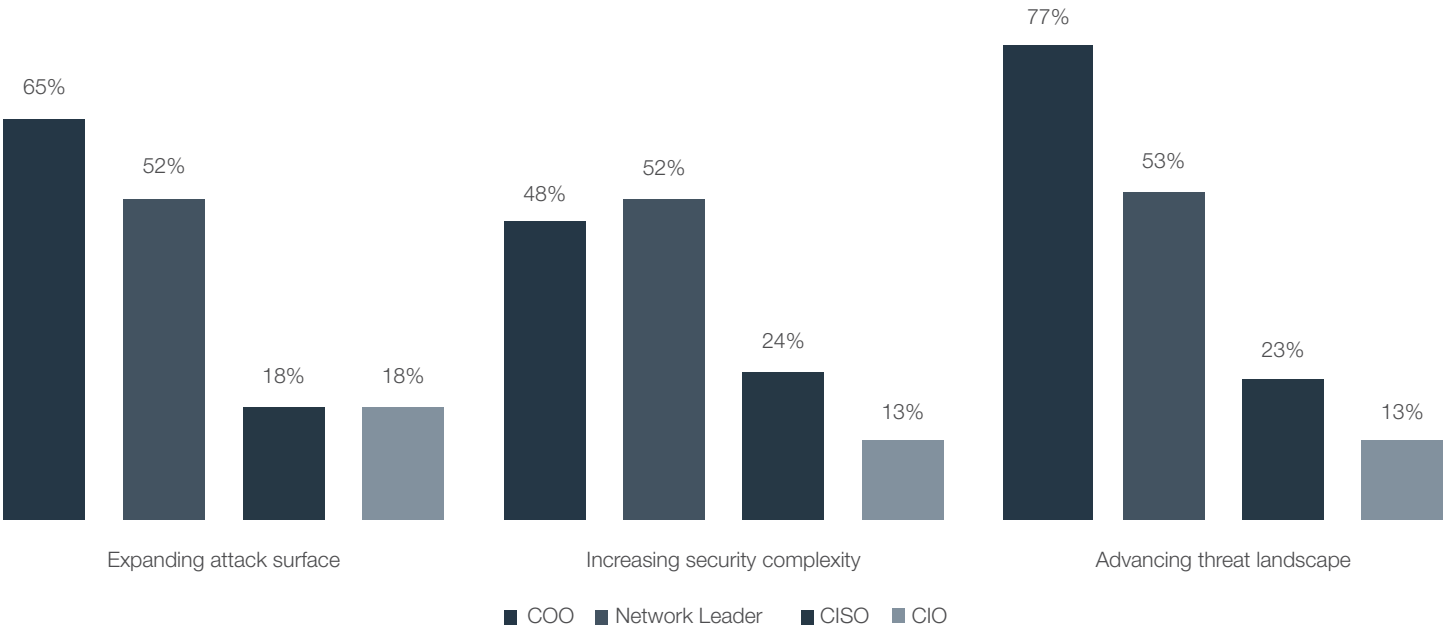


Figure 20: Percentage of respondents citing risk management challenges: COO vs. IT leader vs. CISO.

Best Practices of Top-tier COOs

We compared the survey responses from two subsets based on the number of intrusions experienced. This comparison between "top-tier" and "bottom-tier" respondents identified a number of best practices that top-tier COOs were more likely to employ:

1. Top-tier COOs are 168% more likely to cite regulatory changes as a major success challenge, and 45% more likely to schedule compliance reviews in response.

While respondents cite a number of issues that affect their jobs, the top tier were more than 168% more likely to cite regulatory changes as one of the three biggest issues impacting professional success. In a related finding, top-tier COOs are 45% more likely to conduct regular security compliance reviews, a likely indicator that these COOs are responding to regulatory challenges in a proactive way.

2. Top-tier COOs are 124% more likely to work in organizations in which a C-level executive has the ultimate responsibility for cybersecurity.

Given the increased organizational awareness of the importance of OT security discussed earlier, it is not surprising that high-level responsibility correlates to fewer intrusions. As discussed earlier, many organizations are moving OT cybersecurity responsibility to the CISO, which should pay dividends in the form of fewer intrusions.

3. Top-tier COOs are 79% more likely to rank production floor efficiencies as their top success metrics.

COOs constantly balance their traditional focus on operations with growing expectations for securing the OT infrastructure. Top-tier COOs find ways to meet their security obligations while continuing to focus on operational efficiency.

4. Top-tier COOs are 49% more likely to use multi-factor authentication.

Multi-factor authentication is a proven way to boost an organization's security posture. A recent survey found that security professionals supplement passwords with multi-factor authentication for their personal security more than any other measure.[11] The most successful COOs when it comes to cybersecurity are adopting this best practice and increasingly their threat defenses as a result.

5. Top-tier COOs are 34% more likely to track productivity gains as a cybersecurity metric.

COOs are measured based on productivity, and it makes sense that they would connect security programs with operational efficiencies—whether completing tasks faster or simply avoiding manual workflows by automating them. Top-tier COOs are 49% more likely to track financial implications as a cybersecurity metric.

Organizations routinely grade their COOs on overall financial performance. Therefore, it comes as no surprise that top-tier COOs extend their budget-tracking process to cybersecurity responsibilities.

6. Top-tier COOs are 34% more likely to report the results of penetration and intrusion tests to the person responsible for cybersecurity.

This finding underlines the importance that cybersecurity leaders place on testing as a way to accurately access risk. Testing proactively pinpoints vulnerabilities and provides actionable areas for remediation. The fact that top-tier COOs have time to devote to testing suggests that they have additional staff who can handle the day-to-day security tasks.

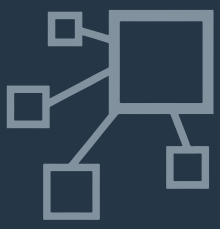
Conclusion

The research shows that when it comes to OT cybersecurity, COOs are both highly visible in the organization and strongly challenged to manage risk and execute their cybersecurity responsibilities in addition to their traditional operational mandates. COOs who seek to improve their security performance can adopt these best practices of their more successful counterparts:

Report and track key security and operational metrics

Conduct regular security tests and compliance reviews

Focus on the financial implications of cybersecurity measures



Invest in proven countermeasures such as multi-factor authentication

References

[1] Barbara Filkins and Doug Wylie, "SANS 2019 State of OT/ICS Cybersecurity Survey," SANS Institute, June 11, 2019.

[2] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 8, 2019.

[3] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[4] Barbara Filkins and Doug Wylie, "SANS 2019 State of OT/ICS Cybersecurity Survey," SANS Institute, June 11, 2019.

[5] "The CFO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, September 11, 2019.

[6] Doug Olenick, "Expanding Attack Surfaces and Difficulties Obtaining The Right People Worry NCSA panelists," SC Magazine, October 16, 2018.

[7] "Cyber Risk Is Top Concern for All, SMB Risks CISOs Need to Heed," The CISO Collective, October 25, 2019.

[8] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[9] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[10] "Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges," Fortinet, September 4, 2019.

[11] "The 2019 State of Password and Authentication Security Behaviors Report," Ponemon Institute, January 2019.

www.fortinet.com

January 4, 2020 12:35AM

D:\Fortinet\Test Report\grey test report\COO and Cybersecurity\report-COO-and-cybersecurity-V2-01420-1234AM

323524-0-0-EN