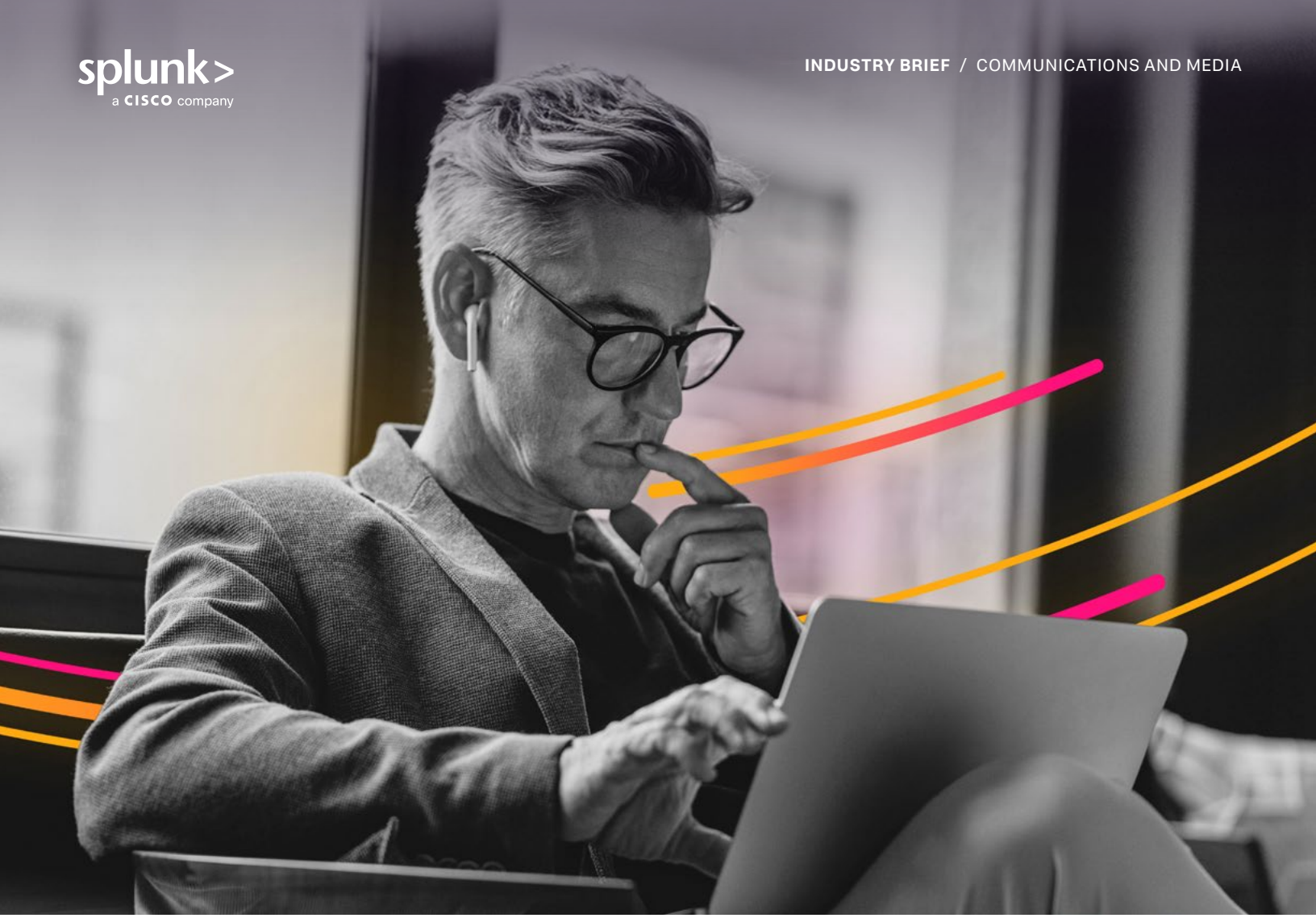

The CISO Action Guide for Communications and Media:

Risk, Resilience, and Regulation in the AI Era

CISOs in the communications and media industry stand at the center of a signal storm of change, and it will only accelerate in the AI era. Yet, they stay resilient in the face of escalating threats to service delivery, rising customer demands, and new pressures around securing AI. They are meeting this moment by: adopting new solutions to strengthen security, collaborating across the C-suite, and boosting team productivity and skills. Data suggests that despite everything coming at communications and media CISOs in the AI era, they are staying in the fight to champion resilience and defend service excellence.

To gain a better understanding of this growing role, we surveyed 650 CISOs globally to see how they are adapting to address the current era. Here, we highlight key findings from respondents in the communications and media industry.

Let's take a look.

79% **of communications and media CISOs report that role responsibilities have become more complex and difficult**

The expanding role of the CISO

The CISO's role isn't just evolving — it's *expanding*. In the communications and media industry, reliable service delivery and security are non-negotiable. CISOs are responsible for protecting customer data, ensuring compliance, and stopping system outages caused by cyberattacks. If that wasn't enough, many are now the de facto AI policy leaders at their organizations. As AI integrates into daily operations across departments, a vast majority (95%) of communications and media CISOs are responsible for AI governance and risk management.

CISOs are also gaining more oversight of the complex mergers and acquisitions process that is becoming common in the telecoms space. Thirty-eight percent noted that they've become responsible for cybersecurity risk assessment and acquisition integration in the last year, adding tasks to CISOs' already full slate.

And who knew CISOs would oversee engineers and software developers? More than three-quarters (80%) of communications and media CISOs report that secure software development (DevSecOps) falls under their purview.

At the same time, they still face an increasingly difficult threat landscape. Today's attacks are far more convincing, and 80% of communications and media CISOs are concerned about their personal liability for cybersecurity incidents. Yet, even with growing risk, only 42% feel they can convince their leadership to increase the security budget when needed.

The CISO's mounting challenges

94% **Growing sophistication of threat actor capabilities**

86% **Increasing pace of technology advancements**

80% **Shifting regulatory requirements**

Respondents who said the challenge was moderate or significant

Shared visions shape strategies

The expanded role of the communications and media CISO places them shoulder to shoulder with their C-suite counterparts. Unsurprisingly, technical C-suite roles like the CIO and CTO are communications and media CISO's closest allies. They are vital partners sharing joint accountability on several business objectives.

Joint-accountability with technical C-suite roles (CIO, CTO, etc.)

Manage security operational business risk	**80%**
Deliver key security initiatives	**78%**
Direct security budget/funding	**78%**
Control security-relevant data access	**70%**
Meet key business initiatives	**55%**

Collaboration across the C-suite doesn't stop there. A majority (69%) of CISOs in communications and media are also working side by side with the CEO on security operational business risk, compared to the 56% average across all industries.

But challenges remain. Eighty-five percent of communications and media CISOs report that cybersecurity fluency among other C-suite leaders is a significant hurdle to collaboration. The answer to that challenge? Data. It's a common tongue that can express the nuances of digital resilience, surface shared risks, drive unified decisions, and lay the foundation for AI governance. This is all the more important when considering that high data volumes were reported as a challenge by 39% of communications and media CISOs, higher than the cross-industry average of 28%.

Adopting a shared data fabric architecture can help communications and media organizations by acting as a connective tissue that harnesses disparate data sources.

The AI imperative

In the communications and media industry, AI adoption is no longer a question of "if," but "how much" and "what kind?"

CISOs in communications and media are ahead of the curve in a few areas when it comes to AI adoption:

- 69% have *fully* adopted embedded AI in vendor tools — compared to 42% across all industries.
- 45% have *fully* adopted automation — compared to 32% across all industries.
- 43% have *fully* adopted machine learning (ML) — compared to 21% across all industries.

While generative AI and agentic AI are in the early stages of adoption, the industry has made more progress than others. In fact, 74% have *partially* adopted generative AI, compared to 38% across all industries. And 89% are in the exploration stage of agentic AI, compared to 39% across all industries.

Security teams view AI as a productivity booster, especially as alert volumes grow overwhelming. Communications and media CISOs use AI to filter noise, identify key threats, and manage information more effectively.

Today's CISO navigates the challenge of embracing AI and setting strong safeguards. For telecoms CISOs, that involves balancing innovation, strict security protocols, and customer satisfaction.

Communications and media CISOs' biggest AI security concerns

1. **Data leakage**
2. **Shadow AI**
3. **Hallucination impacts**

AI enables productivity gains for communications and media security teams

96%
Allows more security events to be reviewed

94%
Improves data correlation from multiple sources

62%
Accelerates execution of basic repetitive tasks

Data includes respondents who somewhat and strongly agree

splunk> a CISCO company

The promise of agentic AI

While the data confirms that communications and media CISOs have not yet deployed agentic AI to a meaningful extent, they do believe it will someday strengthen their security postures and amplify the impact of their teams.

Communications and media CISOs see agentic AI's potential

82% **Increase correlation and response speed**

79% **Increase the amount of data reviewed when threat hunting or correlating IOCs**

73% **Improve security ROI**

Data includes respondents who somewhat and strongly agree

But despite agentic AI's potential, CISOs are not blind to the inherent risks. Their enthusiasm is paired with smart skepticism, rooted in very real concerns about the technology's autonomous nature. Communications and media CISOs overwhelmingly rank hallucination impacts, like missed alerts or false positives, as their number one concern about adopting agentic AI for cybersecurity.

AI risks also come in the form of more sophisticated external threats. CISOs see agentic and non-agentic AI as enhancing adversaries' capabilities, with AI agents amplifying attack quality and impact rather than helping generate more attacks.

Communications and media CISOs sound the alarm on AI-driven threats

	A top concern for agentic AI	A top concern for non-agentic AI
Increased sophistication of social engineering attacks	**91%**	**93%**
Increased deployment speed and complexity of persistence mechanisms	**85%**	**14%**
More rapid proliferation of exploits	**72%**	**99%**

Respondents could select top 3 options

CISOs choose talent over tech

Although communications and media CISOs are exploring how AI agents can help increase detection speed, they emphasize that technology won't replace security analyst jobs. Instead, they are investing in people by upskilling their current workforce, adding full-time security talent, and leveraging contractors, recognizing the value of specialized expertise.

In fact, only 2% of communications and media CISOs responded that they are addressing talent gaps with technology investments, like AI or automation. However, over half (57%) of respondents expect that *some* of their skills gaps will remain unfilled.

57% **of communications and media CISOs surveyed expect *some* of their skills gaps will remain unfilled**

Measuring security success

Communications and media CISOs are starting to reframe security as a mission enabler rather than a cost center. But only 41% of these CISOs report that they can directly correlate ROI to risk mitigation and remediation activities.

On a positive note, communications and media CISOs are adopting more meaningful measures of success — with 85% ranking incident reduction as the most critical outcome for communicating ROI to peers. Showing fewer incidents helps the C-suite and board see how the company is preventing service downtime, reputational damage, and other costly consequences of a major breach.

There is still a significant gap in communicating impact on key metrics such as cost reduction or customer satisfaction, even though uptime and data security are directly connected to these. Poorly communicating security's value can create a fundamental misunderstanding of achievable goals. For example, 80% of communications and media CISOs say leadership sets unrealistic expectations around the revenue impact of security events.

Successful communications and media CISOs use data-driven narratives to reframe security spending as a strategic investment for secure innovation, with the payoff especially clear in compliance: A majority (93%) believe that their leadership or board sets realistic objectives for adherence to regulatory requirements — a win in an industry where compliance can make or break service deployment.

Find out more in **The CISO Report** about how Splunk can help CISOs build a path to digital resilience.

Get the full report >

Communications and media overview >

85% **rank incident reduction as the most critical outcome for communicating ROI to peers**

93% **believe that their leadership or board sets realistic objectives for adherence to regulatory requirements**

Communications and media CISOs can meet the moment

In a sector defined by constant advancement, today's communications and media industry CISOs can rise to the challenge and help their companies lead in the AI era.

Are you up to the challenge? Here are a few ways that communications and media CISOs can enhance enterprise risk and resilience:

Question to ask	How do I compare?	How can I take action?
Am I clearly demonstrating security's strategic value to the full leadership team? Yes: ☐ No: ☐	**41%** of communications and media CISOs can directly correlate ROI to risk mitigation.	☐ Translate security benefits into a language the rest of the organization understands. ☐ Map security initiatives to organizational outcomes. ☐ Invite colleagues to table-top exercises.
Do we have systems in place that focus on the quality of security initiatives? Yes: ☐ No: ☐	**77%** of communications and media CISOs see a lack of shared data views or operating layers as a challenge in improving data management.	☐ Leverage automation to filter out alert noise. ☐ Shift the mandate from alert quantity to investigation quality. ☐ Focus on impactful metrics like detection quality.
Am I seeking opportunities to collaborate with my non-technical C-suite peers? Yes: ☐ No: ☐	**78%** of communications and media CISOs share joint accountability with technical C-suite roles on key security initiatives.	☐ Establish a shared planning cycle to embed security into business strategy. ☐ Build joint accountability on key initiatives and KPIs. ☐ Establish security as a core driver of business success.
Are we maximizing my organization's AI capabilities? Yes: ☐ No: ☐	**94%** of communications and media CISOs believe AI improves the ability to correlate data from multiple sources.	☐ Champion a clear AI governance, privacy, and accountability strategy. ☐ Build comprehensive guardrails for private data usage. ☐ Keep humans in the loop for critical decisions.
Are we leveraging AI tools to free up our team from routine tasks? Yes: ☐ No: ☐	**69%** of communications and media security teams have experienced *moderate* to *significant* burnout over the past 12 months.	☐ Automate routine detection and response tasks to free up analysts. ☐ Pair machine precision with human intuition and creativity. ☐ Build an environment where AI augments human expertise.

If you answered "no" to any of these questions, we're here to help. Contact us now to learn how you can build a more resilient business.

Learn how Splunk is helping communications and media CISOs develop leading security and observability practices.

splunk> a CISCO company

www.splunk.com