Securing cutting-edge content from high-tech attacks

TCS Risk & Cybersecurity Study:
Media & Information Services Report

Securing cutting-edge content from high-tech attacks

The media and information services industry seeks the widest possible audience. But are we prepared for the unwanted guests?

Whether the media and information services industry has undergone the most seismic shifts in recent years, or whether it just seems that way because it's the industry that communicates such business developments in every industry, no one can deny that media and information services companies have experienced disruption, changes to business models and consumer behavior, large-scale mergers and acquisitions, and even redefinition and recategorization in recent years. And with each of those comes new and different cyber threats that make earlier precautions put in place seem quaint and naïve, if not misguided and counterproductive.

Securing cutting-edge content from high-tech attacks

What once seemed a largely simple-to-define industry has morphed and moved in unexpected directions and changed into unforeseen shapes over the past decade:

- The rise of video streaming platforms like Netflix, Amazon Prime Video, Disney+, and Hulu transformed the way people consume media. This has led to a decline in traditional cable TV subscriptions as more consumers “cut the cord.”
- Music streaming platforms like Spotify, Apple Music, and Tidal have gained immense popularity, resulting in the decline of physical music sales and even downloads.
- The global video games market, already huge and spurred to greater popularity as a result of COVID lockdowns, was valued at $184 billion by the end of 2023, which is now larger than the movie and music industries combined.[1, 2]
- Thanks to the extensive use of data analytics, media customers now expect personalized content recommendations that reflect their unique tastes and interests.
- User-generated content has become the engagement model for everything from YouTube to Tik-Tok, Instagram to Substack.

And even these major shifts only scratch the surface of the changes impacting the industry, whether it be in the area of artificial intelligence (a point of contention in the 2023 screenwriters’ strike) or multifactor authentication (MFA) and machine learning, which streaming services are using to reduce the number of shared passwords impinging on their revenue.[3]

Methodology at a Glance

The TCS Risk & Cybersecurity Study surveyed Chief Information Security Officers (CISOs) and Chief Risk Officers (CROs) via survey and in-depth interviews amid an unprecedented upsurge in increasingly sophisticated cyberattacks. The survey respondents were drawn from 607 North American, European, and UK-headquartered companies in four industries: media and information services, banking and financial services, manufacturing, and utilities. These industries are facing an unprecedented range of cyber threats and increased risks to business data, customer data, operations, trade secrets, and supply chains.

In this report, we examine the greatest security risks media and information services (MIS) firms face, explore how effectively these 76 CISOs and 75 CROs are creating security strategies, and offer suggestions for improvement based on our domain expertise in the media and information services industry worldwide.

Securing cutting-edge content from high-tech attacks

Industry cybersecurity and risk trends

The media and information services industry faces a rapidly evolving landscape shaped by technological advancements and changing cyber threats.

1. **A changing regulatory landscape.** Legislators worldwide increasingly require businesses to demonstrate competency in managing cybercrime risk. Regulations like the NIS 2 Directive (EU 2022/2555), advanced certification requirements like Cyber Essentials Plus (UK CE+), and the National Institute of Standards and Technology's Cyber Security Framework 2.0 (US NIST CFS 2.0) are mandating effective policies related to information security, cybersecurity, and cryptography management. Companies must demonstrate robust security in their networks and supply chains, report cyber incidents in a timely manner, ensure cyber resilience through business continuity measures, and appropriately manage user access controls supported by MFA.

2. **Traditional security threats.** Historically, the biggest security threats for media and information services companies have stemmed from three factors: hackers and thieves seeking to expose data for profit or to compromise businesses; corporate espionage; and lack of employee awareness regarding basic security measures like password safety and phishing prevention. As communications operations increasingly provide the backbone infrastructure for digital services, they become both attractive targets and potential platforms for launching attacks on digital media companies. They must ensure there are no exposed vulnerabilities from Internet-of-Things (IoT) architectures, untrained users, or third-party partners.

3. **Digital identity at the core.** As the physical and digital worlds converge, digital identity will be central to the next wave of business disruption. Communications carriers, holding a higher trust quotient with consumers compared to cloud hyperscalers, have the potential to play a foundational role in areas like decentralized identity, trusted identity, and access management ranging from e-signatures to AV/VR identification. Carriers must embrace the responsibilities that come with these opportunities.

4. **Accelerated adoption of AI and cloud.** The industry is witnessing a surge in artificial intelligence (AI) adoption to predict usage patterns in equipment operations and customer interactions, especially for virtual assistants and chatbots. Cloud technologies and services are also seeing a spike in usage as they streamline tasks, reduce costs, and mitigate cyber risks. However, uncertainties around future AI legislation and policy divergence between countries raise concerns about potential innovation roadblocks. (See the TCS AI for Business Study at **on.tcs.com/2024-global-AI-study** for more findings about communications, media and information services executives' attitudes and plans regarding AI today.)

Securing cutting-edge content from high-tech attacks

In the TCS Risk & Cybersecurity Study, two distinct groups emerged from our research among media and information services CISOs and CROs: **Pacesetters,** whose companies reported higher than industry averages for both revenue growth and profit growth over a four-year period (12% of MIS firms surveyed), and **Followers,** who reported lower than average revenue and profit growth during that period (44% of MIS firms surveyed).

Here's what our survey found:

1 Only among MIS Pacesetter firms do executives feel as confident about avoiding a major cyber incident as the CISOs and CROs in other industries feel.

2 Digital threats to the production environment ranks as MIS CROs' number one cyber concern. Their companies' digital ecosystem partners are also far more likely to drive the need for risk management than is the case in other industries.

3 MIS CISOs and CROs are more likely to cite "competing interests for board or senior leadership" as an obstacle to cybersecurity and risk mitigation initiatives than are those executives in other industries.

4 Board-level discussions on cyber risk and security issues take place less frequently at media firms, and MIS C-suites are less likely to be proactive on cyber issues compared to their counterparts in other industries.

5 CISOs and CROs at MIS companies that embrace cloud platforms because of — not despite — their cybersecurity capabilities also express far higher levels of confidence in their overall position regarding risks and threats.

Risks, threats & targets

The industry's distinctive nature extends into its cybersecurity concerns.

The digital transformation of the media and information services industry has brought forth myriad new business and operating models, but with them arrived an array of risks. While these companies share many of the same cyber risk and security challenges that other industries face, they also grapple with unique challenges that are particularly or especially pertinent to the MIS sector:

Intellectual Property Theft: MIS companies produce valuable intellectual property, including movies, TV shows, music, and other content, which cybercriminals target to steal and distribute without authorization, often before the official release, leading to financial losses and reputational damage for these firms.

Fake News and Disinformation: MIS companies can be the target of disinformation campaigns where attackers may try to compromise platforms to spread fake news or manipulate public perception. And AI tools can now be used to create "deepfakes" or alter existing media in misleading ways. This leads to risks both in terms of content integrity and the potential spread of misinformation.

Personally Identifiable Information: Oceans of user data (including content preferences and even user-to-user interactions) combined with privacy regulations differing by country or region adds to an already complex web of cyber risk mitigation for MIS companies.

Distributed Denial of Service (DDoS) Attacks: High-profile media platforms can be targeted by DDoS attacks, either for ideological reasons, extortion, or simply to cause disruption.

Supply Chain Attacks: Many MIS companies rely on third-party vendors for post-production, special effects and other services. Vulnerabilities in these vendors can provide a backdoor to the main company's assets.

Risks, threats & targets

In the MIS industry, CISOs grapple with a diverse array of cyber risks and security concerns. Advanced social engineering attacks top their list, with techniques like watering hole, pretexting, and whaling to exploit human psychology to breach defenses (see Figure 1). These attacks pose significant threats in an industry where individuals frequently exchange personal and proprietary information, often bypassing traditional security measures by manipulating people rather than targeting technological vulnerabilities.

Attacks leveraging AI and machine learning closely follow as major concerns, reflecting the industry's increasing reliance on these technologies for content creation, recommendation systems, and user engagement. While AI enhances cybersecurity measures, attackers also weaponize it to launch more sophisticated and automated attacks. AI-driven malware adapts to evade detection, and AI can automate the creation of highly convincing phishing schemes. This dual nature of AI highlights the need for robust governance and advanced defense mechanisms to counteract evolving threats.

Web cache poisoning ranks third, emphasizing the industry's dependence on web-based services and the potential disruption from corrupting cached data. This attack vector can lead to widespread dissemination of malicious content, redirecting users to malicious sites or serving altered information. Given the industry's reliance on real-time information delivery, web cache poisoning can profoundly impact service integrity and user trust.

Chatbots and open-source exploitation share the fourth rank. Chatbots, increasingly used for customer service and content delivery, face risks from prompt injection attacks, where malicious actors manipulate the chatbot's responses or behavior. Open-source exploitation targets vulnerabilities in widely used software, integral to many media and information services platforms. The pervasiveness of open-source tools means a single exploit can have widespread repercussions across the industry.

Tactics which most concern CISOs when thinking about cybersecurity between now & 2025	Media & information services *n = 76*	Other industries *n = 230*
Advanced social engineering attacks (watering hole, pretexting, whaling, etc.)	1	1
Attacks leveraging AI/machine learning	2	2
Web cache poisoning	3	6
Chatbots	4	8
Open-source exploitation	4	3
Crime-as-a-Service	6	4
Botnets	7	7
Over-the-air (wireless chip) exploits	8	5

Figure 1

While ranked lower, Crime-as-a-Service (CaaS) and botnets remain significant threats. CaaS lowers the entry barrier for cybercriminals, potentially increasing the frequency and diversity of attacks against MIS companies. Botnets continue to evolve, posing risks to content delivery networks and user data through large-scale DDoS attacks, data theft, and malware distribution.

Risks, threats & targets

Over-the-air (wireless chip) exploits, though ranked eighth, reflect concerns about the security of wireless communications. These exploits target devices like smartphones, smart TVs, and IoT devices, which are ubiquitous in media and information services and often contain sensitive information or serve as gateways to other content and services.

Beyond these top-ranked concerns, the industry faces additional cybersecurity challenges. Digital rights management (DRM) remains critical, especially as AI advances make it easier to circumvent protections, threatening copyright and intellectual property. Advanced Persistent Threats (APTs) pose long-term risks to intellectual property, strategic plans, and sensitive communications, particularly for companies involved in investigative journalism or operating in politically sensitive environments.

The rise of AI in content creation and distribution raises complex questions about copyright and human rights. MIS companies must protect their intellectual property while ensuring their use of AI doesn't infringe on others' rights. Furthermore, the potential for AI systems to be used for mass surveillance, content manipulation, or the spread of misinformation presents serious ethical and human rights concerns that responsible organizations must address.

Algorithmic bias in content distribution and elevation presents both ethical and security challenges, potentially exposing MIS companies to reputational damage and regulatory scrutiny. This issue intersects with broader concerns about the integrity of information services and the potential for skewed or discriminatory content delivery.

In this complex threat landscape, media and information services CISOs face the daunting task of protecting their organizations against a wide array of evolving threats while ensuring the free flow of information and creativity that fuels their industry. Addressing these challenges requires a holistic approach that combines advanced technological defenses with robust governance, continuous monitoring, comprehensive threat intelligence, and a keen awareness of emerging threats. By implementing multi-faceted strategies that include technical solutions, employee education, ethical guidelines, and a commitment to transparency and user privacy, the industry can better navigate the ever-changing cybersecurity terrain.

Risks, threats & targets

In our survey, media and information services CROs also identified several pressing cyber threats that they think could have a significant impact on their operations (see Figure 2). Topping the list is the threat of Distributed Denial of Service attacks targeting the production network. Unlike distribution networks which disseminate content to the public, the production network is the backbone of content creation. A successful DDoS attack here could halt the creation process, leading to significant financial and reputational losses.

Second, the public exposure of sensitive information, such as emails and confidential legal contracts, is a looming threat. A notable example is the Sony Pictures hack in November 2014, where a massive amount of confidential data, including personal emails and unreleased films, were leaked. Such incidents not only tarnish a company's reputation but can also lead to legal repercussions. Furthermore, in a world where email has replaced the phone as a primary means of business communication and social media is central to marketing campaigns, the impersonation of high-profile individuals — be it executives, celebrities, or news figures — poses a significant risk. Hackers can leverage these impersonations to spread misinformation, manipulate stock prices, or even commit fraud.

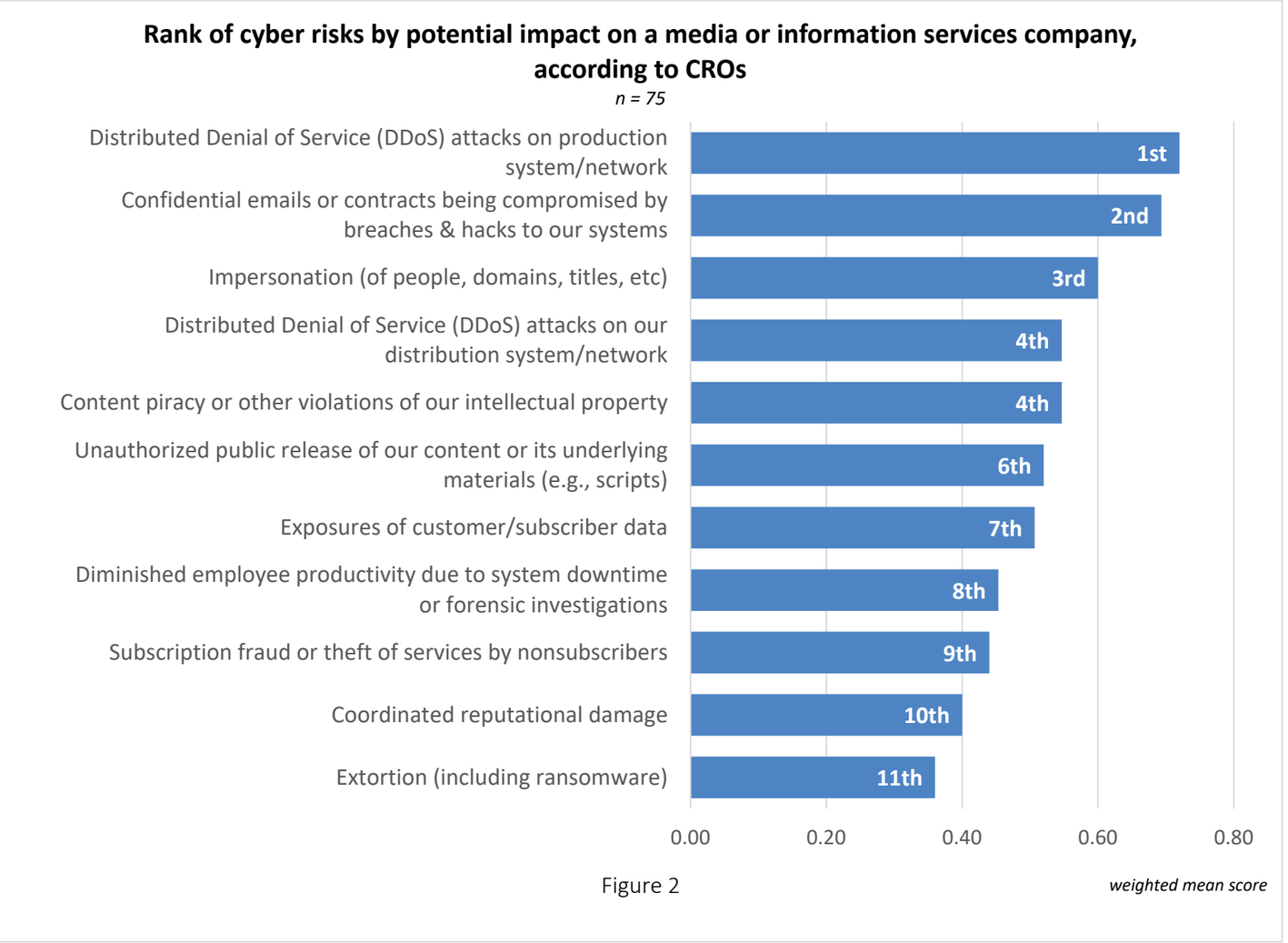


Figure 2

Risks, threats & targets

More broadly, the digital, often decentralized nature of content development and distribution drives risk management initiatives for media and information services CROs to a greater extent than in other industries with more traditionally defined boundaries. In the interconnected MIS industry, companies often collaborate with a range of ecosystem partners, from suppliers and collaborators to distributors. When we asked CROs across industries what broad groups of stakeholders tended to drive demand for risk management at their companies, MIS CROs were far more likely to rank "ecosystem partners" as a leading determinant (see Figure 3).

This interconnectedness, however, also amplifies cyber risks. According to the survey data, MIS CROs rank the risks associated with these ecosystem partners as their 4th greatest driver for risk management. This is in stark contrast to CROs in other industries, who together ranked it 8th. This highlights the unique vulnerability of the MIS industry due to its reliance on a wide range of external partners.

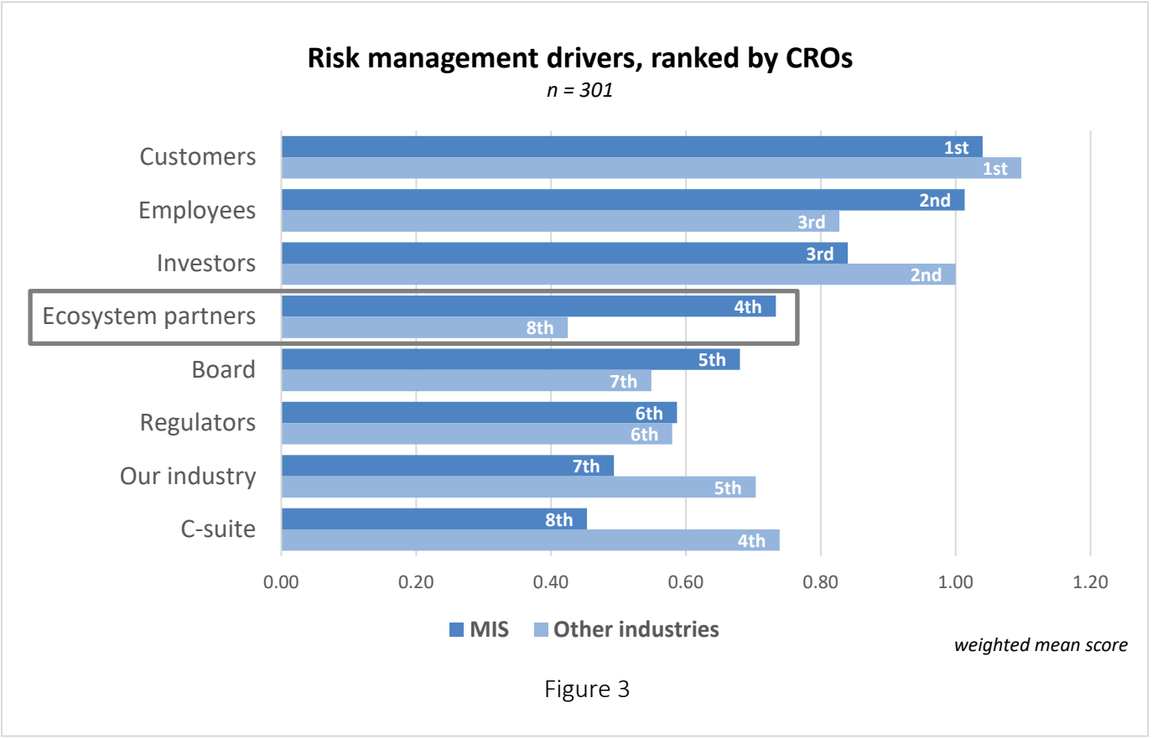


Figure 3

While "regulators" were ranked no higher by MIS CROs than those in other industries as causing demand for increased cyber risk management, in TCS' experience the risk represented by "customers" can include risks to their own private data; risks to a company putting that data to use (for recommendation purposes, for example), which may be governed very differently depending on the country or region; and the IP or legal risks inherent in content license agreements, which can be governed under different terms and conditions for different levels of subscribers and which often vary by country — all made more complex by the widespread use of VPNs and other methods of accessing content (including account/identity theft) in countries for which it is not licensed or permitted.

Risks, threats & targets

For their part, MIS CISOs rank “intellectual property” and “personally identifiable information” as their most time-consuming activities (see Figure 4) compared to “strengthening our corporate systems — email, payroll, legal — against incursions” (which ranked 5th) or “protecting/monitoring our vendors’ and third-party suppliers’ systems” (6th). Like their CRO counterparts’ concern about the effect a DDoS attack could have on their production network (as shown in Figure 2), MIS CISOs are also actively engaged in avoiding downtime caused by breaches and attacks, ranking such problems as their third-most time-consuming issue.

Most time-consuming activities related to information security for media & information services CISOs	**Media & information services** *n = 76*
Protecting intellectual property & sensitive data	**1**
Protecting the reputation or personally identifiable information (PII) of high-profile individuals associated with our company or its content	**2**
Avoiding downtime caused by breaches & attacks	**3**
Improving operational efficiency	4
Strengthening our corporate systems (email, payroll, legal, etc.) against incursions	5
Protecting/monitoring our vendors’ & third-party suppliers’ systems	6
Enabling & protecting employee access to our systems & facilities	7
Protecting the reputation of our corporation (or subsidiaries)	8
Demonstrating compliance with privacy & cybersecurity regulations	9
Protecting our distribution network(s)	10

Figure 4

Leadership challenge

Cyber risk and security leaders' challenges can also come from other leaders.

Recent workplace changes (such as work-from-home during the pandemic) have been the greatest obstacle to implementing new cyber risk and security initiatives, according to both MIS CISOs and CROs. (In other industries, this was ranked 3rd; see Figure 5.) MIS executives also indicate their corporate leadership thinks less strategically about cyber risk and security. MIS cyber executives' 3rd highest ranking obstacle to cyber initiatives was "lack of collaboration across business units"; for those in other industries, this problem only ranked 9th. Similarly, MIS initiatives are far more likely to be derailed or ignored due to "competing interests for the board or senior leadership."

The greatest challenges to cybersecurity & risk mitigation initiatives according to CROs & CISOs	Media & information services *n = 151*	Other industries *n = 456*
Workforce changes/requirements (work from home, bring-your-own-device, etc.)	1	3
Assessing cyber risks & quantifying relevant costs	2	2
Lack of collaboration across enterprise units (business, IT & security)	3	9
Skill sets to manage, engineer & support cybersecurity technology	4	1
Budget constraints	5	10
Competing interests for the board or senior leadership	6	11
Accumulated complexity of our own business processes & operations	7	5
Reliance on legacy IT systems	8	3
Difficulty in demonstrating return on cybersecurity investments	8	6
Lack of staff diversity (including of thought & experience) to assess risks & threats	10	7
Difficulty in mandating that our vendors adopt advanced technologies & policies	11	8
Outdated, siloed & non-integrated security tools	12	12

Figure 5

Leadership challenges

In a variety of other ways, MIS CISOs and CROs continued to indicate less engagement on the issues of cyber risk and security among their companies' senior leadership.

For example, at MIS companies, securing against and mitigating cyber risks comes up less often at board-level meetings than it does in the other industries we surveyed (see Figure 6). Only among the more financially successful MIS firms – the "Pacesetters" – did boards discuss cyber risk and security with anywhere close to the frequency of companies in other industries. Another set of Pacesetter companies, however, were the most likely in the MIS industry to "almost never or never" have board discussions on the issue. (Pacesetter MIS executives were eight times more likely to say their own board basically ignores the issue than were executives at Pacesetter firms in other industries.)

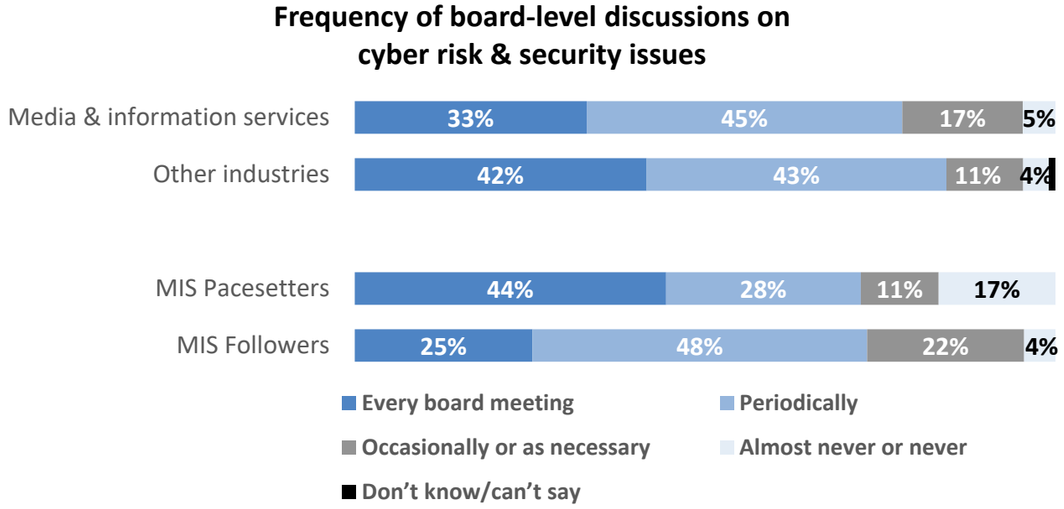


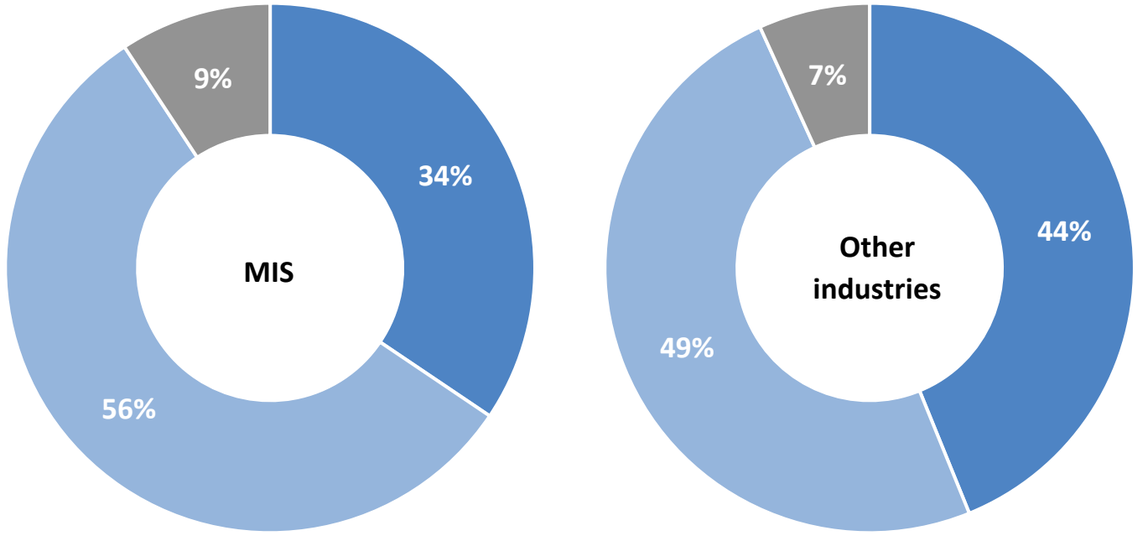
Figure 6

Leadership challenges

Similarly, compared to answers from executives in other industries, media and information services CISOs and CROs are less likely – by 10 points – to say their fellow C-suite officers are proactive on cyber issues (see Figure 7).

Why this short-sightedness on the part of C-suites in an industry built on creativity, imagination and ideas? For one, despite large-scale mergers and acquisitions on a financial basis, many MIS companies prefer to operate in a decentralized manner, with various business units or studios working semi-independently. This can lead to challenges in establishing a unified cybersecurity strategy across the entire organization.

Attention given to cyber risk & security issues by other C-suite & business unit leaders



PROACTIVE:
Our C-suite & business unit executives actively & frequently discuss our cyber risks & security

REACTIVE:
Our C-suite & business unit executives discuss cyber risks & security only when cyber threats are brought to their attention or only after a cyberattack hurts our business

DISENGAGED:
Our C-suite & business unit executives have hardly addressed cyber risk & security

Figure 7

Leadership challenges

Similarly, the creative and open culture prevalent in many MIS companies might sometimes be at odds with strict cybersecurity protocols. C-suite executives might prioritize fostering creativity over implementing stringent security measures. Additionally, producing content, especially high-quality productions, can be capital-intensive. C-suite executives might allocate more resources to content creation and marketing, viewing cybersecurity as a secondary investment.

This issue of capital priorities competing for cyber risk mitigation seems borne out by the data. Not only are MIS CROs and CISOs more likely to say budget considerations are a leading challenge to implementing cyber risk and security initiatives compared to their counterparts in other industries (see Figure 5), these MIS cyber executives were less likely to see budget increases in their last cycle and more likely to see budgets cut (see Figure 8).

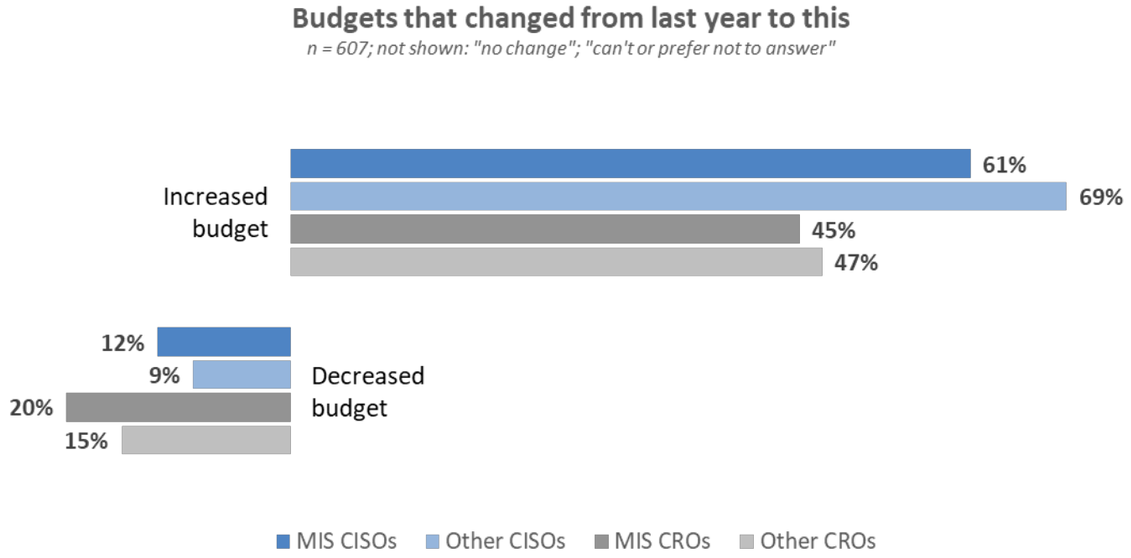


Figure 8

The imperative of identity management

The MIS industry exhibits a dichotomy in its approach to identity management.

While the production environment is fortified with robust security measures like two-factor authentication to prevent unauthorized access, the customer-facing side often relies on basic email and password logins. This simplistic approach caters to customers seeking hassle-free access to content but inadvertently encourages the sharing of login credentials. Netflix had gained nearly 55 million new subscribers by June 2024, two years after it started a concerted effort to crack down on password sharing.[4] However, MIS companies continue to prioritize customer convenience, in contrast to the tighter security measures seen in production environments.

The TCS survey data seems to show evidence of this split. The emphasis on improving identity management is notably higher among CISOs in the MIS industry (see Figure 9), underscoring the criticality of secure authentication, especially in the production realm of this highly digitized sector.

CISOs' budget priorities	Media & information services *n = 76*	Other industries *n = 230*
Data protection & privacy	1	1
Identity management	2	6
Cloud security management	3	2
Emerging security technologies (such as decentralized identity, 5G security, etc.)	4	3
Governance, risk & compliance	5	8
Threat management (including ransomware protection)	6	5
Vulnerability remediation automation	7	7
Advisory consulting	8	10
Managed detection & response	9	4
Operating technology (OT) security	10	9

Figure 9

The imperative of identity management

At the same time, while CISOs in other industries are leaning towards adopting zero-trust or similar advanced security solutions, MIS industry CISOs appear more focused on bolstering foundational security practices, such as patching vulnerabilities and enhancing their digital environments (see Figure 10).

In a similar vein, CROs in the MIS sector are far more concerned about risks to their production ecosystem than to their distribution ecosystem — even though the industry has been shifting from vertical integration in production (witness the number of company credits at the start and end of most movies, for example) to vertical integration in distribution where the parent company owns all (such as Comcast's Peacock) or a major stake (such as Xumo, a 50/50 joint venture between Comcast and Charter Communications) in the consumer platform. As shown earlier in Figure 2, MIS CROs are more concerned about attacks on their production environment than about other cyber risks such as attacks on their distribution environments or content piracy (1.3X more) or subscription fraud (1.4X more).

CISOs' work priorities	Media & information services *n = 76*	Other industries *n = 230*
Enhancing security governance & risk management (e.g., assessing the security posture of the company, defining controls & standards, etc.)	1	1
Strengthening enterprise-wide cyber hygiene (patching, hardening, etc.)	2	8
Establishing a more robust cybersecurity strategy	3	2
Enterprise-wide employee awareness & training	4	6
Security talent acquisition & development	4	3
Managing ecosystem & supply chain risks	6	9
Executive/board mandates on cybersecurity risks	7	5
Regulatory or industry compliance mandates	8	7
Outsourcing our security operations	9	10
Implementing models like "zero trust"/perimeterless security	10	4

Figure 10

Cyber confidence for MIS executives

A lack of support can lead to a lack of confidence.

Given the lower level of support MIS CISOs and CROs feel they get from their corporate leadership, the MIS sector also faces a unique challenge when it comes to cybersecurity confidence.

Notably, the CISOs and CROs within this industry express lower confidence in their ability to prevent major cyber incidents that could lead to reputational or financial damage. Only half of the CISOs and CROs in the MIS sector report feeling confident or very confident about avoiding such incidents. In contrast, nearly two-thirds of their counterparts in other industries express a higher degree of confidence (see Figure 11).

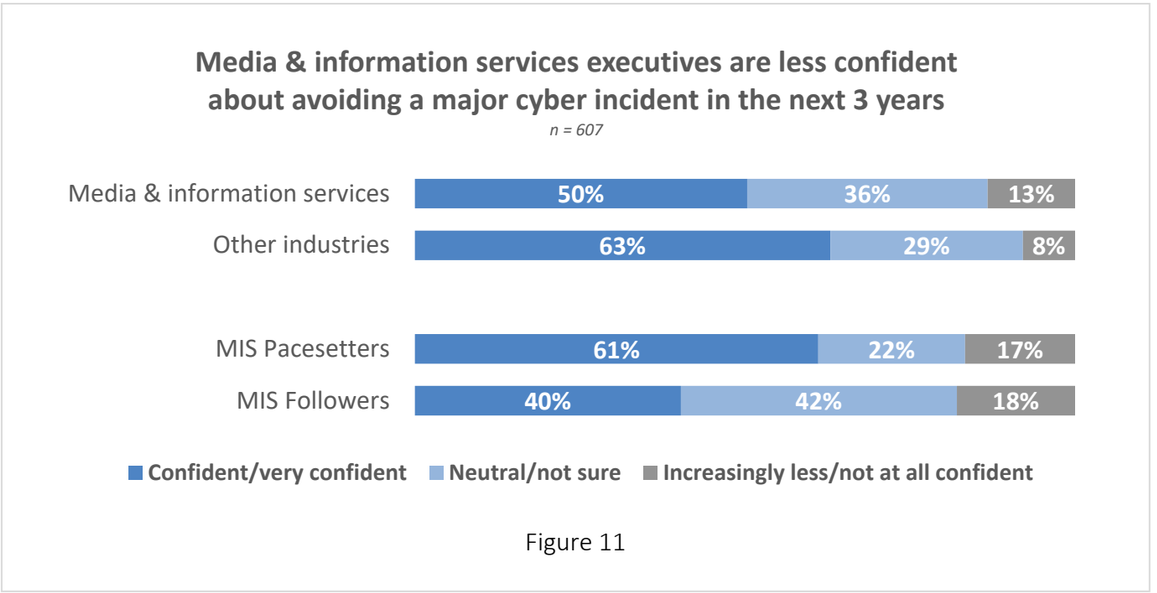


Figure 11

Cyber confidence for MIS executives

Additional evidence comes from the media and information services CISOs, who were asked about their confidence in the cybersecurity technology they are applying against cyber threats. Only 36% of MIS CISOs said they were successfully combating the most sophisticated attacks that are becoming more frequent, compared to almost half of CISOs in other industries who said that their cyber capabilities were successfully combating such threats (see Figure 12).

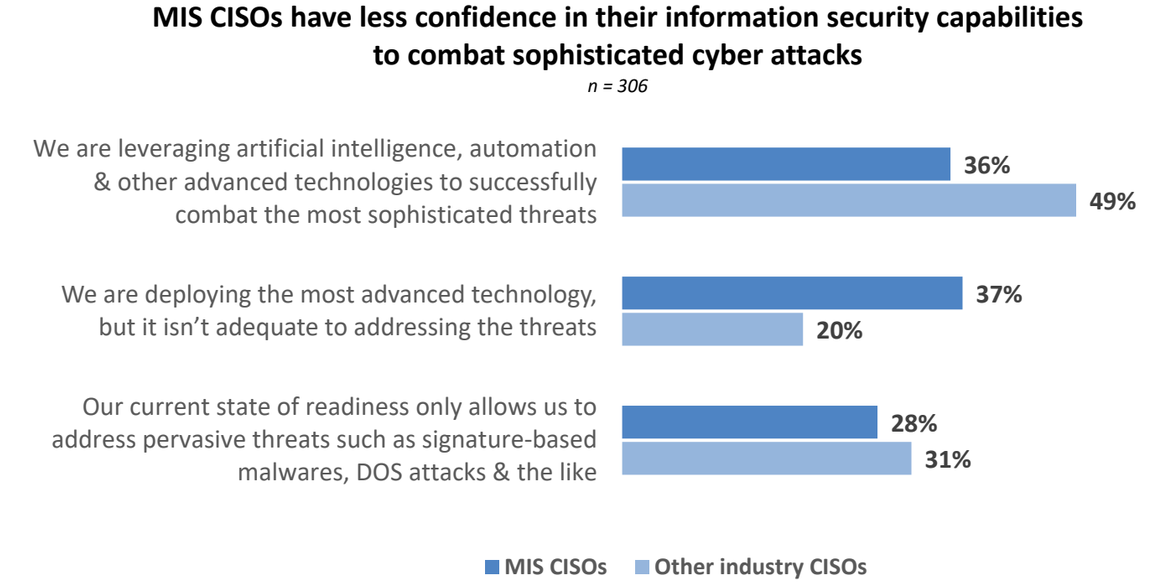


Figure 12

Cyber confidence for MIS executives

Despite the broad digitization of its products and sales, the media and information services industry still lags far behind other industries in its adoption of cloud platforms for operations, production, and distribution, in all the guises those take across the diverse business models and content types of the MIS industry. The TCS Cloud Study[5] found that a quarter of MIS company executives surveyed were “fully cloud-native and modernized,” using “microservices or fully public or fully hybrid cloud models,” compared to 27% who said so across the entire mix of industries surveyed. But in general, most MIS companies are even further behind in their cloud journey. In that study, less than half (44%) of MIS executives said their companies were either fully cloud-native or have achieved cloud-based goals for most of their critical apps and workloads, while across all industries, nearly two-thirds of respondents (65%) said their companies were fully or mostly cloud-based. In fact, no other industry ranked as low in its adoption of cloud platforms.

Perhaps unsurprisingly then, in this more focused study on risk and cybersecurity, MIS executives were no more likely to ascribe cybersecurity benefits, specifically, to using cloud platforms and services than were those in other industries. Among the more financially successful MIS companies, however, a clear preference for cloud platforms’ security emerged (see Figure 13).

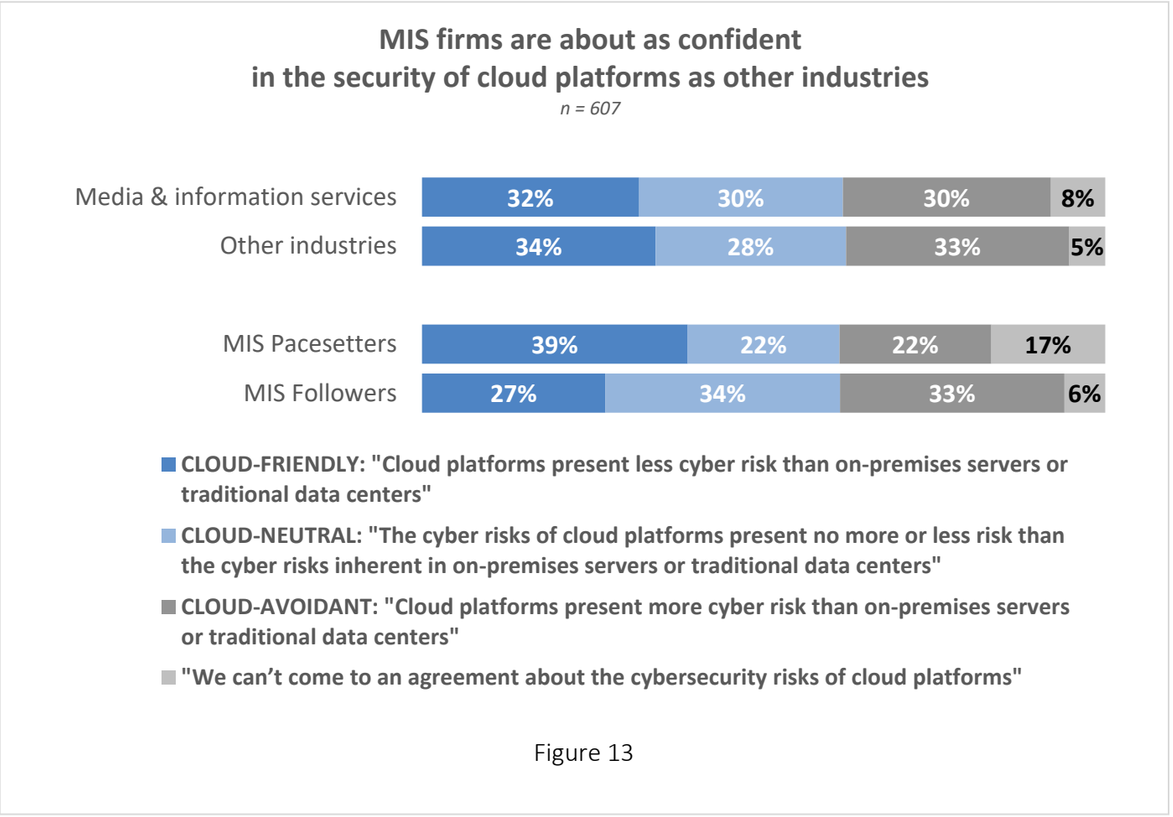


Figure 13

Cyber confidence for MIS executives

On a brighter note, there's a silver lining in the cloud, as the saying goes. Cloud security capabilities have indeed emerged as a game-changer for the MIS industry. Firms that have embraced cloud platforms and cloud-enabled services *because of*, not despite, their cybersecurity capabilities feel they are reaping the benefits. These companies are nearly twice as likely to feel that they have cyber threats well under control compared to those that are hesitant or avoidant of cloud technologies: 45% vs. 22% (see Figure 14).

Embracing cloud-based security not only offers enhanced security features but also positions MIS companies at the forefront of technological innovation, ensuring they remain competitive and resilient in the face of evolving cyber challenges.

Cloud-friendly MIS firms' CISOs & CROs are twice as likely to have greater confidence in their position toward cyber risks & threats than those at cloud-avoidant media companies

n = 139; not included: can't come to an agreement about the security of cloud

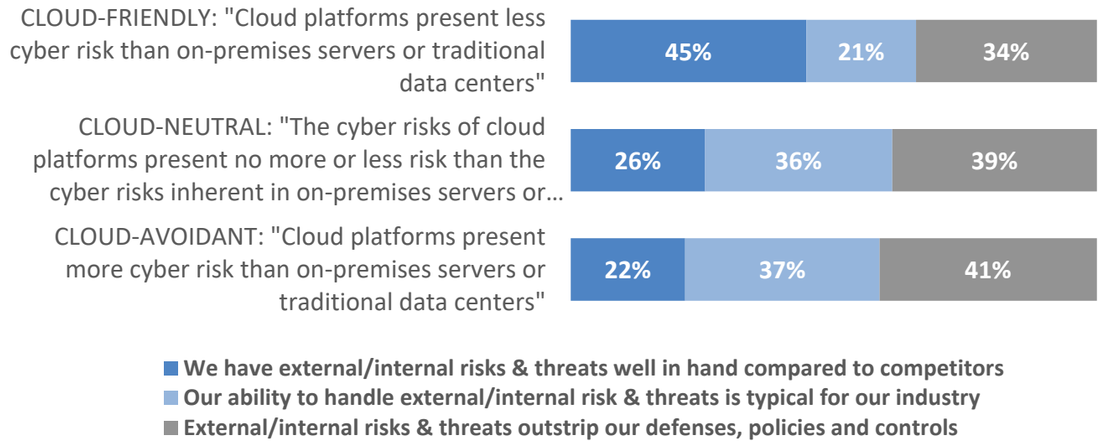


Figure 14

The attention-getters need to pay attention

The MIS industry has some catching up to do to be more cyber secure. Fortunately, there are some solid recommendations where they can start.

The media and information services industry faces various risks, including financial fluctuations, changing consumer preferences, and the pressing need for fresh content. Additionally, there are concerns about privacy, data breaches, and cybersecurity threats. Historically, the MIS sector hasn't been at the forefront of embracing cybersecurity, despite its evident risks.

Yet the threat of cybersecurity breaches is growing. MIS entities manage vast amounts of confidential data, making them prime targets for cyber-attacks. Such incidents can result in substantial financial losses, damage to reputation, and legal consequences.

In addition, media and information services companies are as interconnected in the wider digital ecosystem as any industry. The widespread outages caused by a faulty update to CrowdStrike software in July 2024 — which wreaked havoc on banks, airlines, and healthcare companies — also took many services and productions of major media companies like ESPN, Paramount, Sky News, TF1 and Canal+ offline. Nevertheless, there's a noticeable lack of emphasis on cybersecurity among MIS leaders. Several factors might explain this. The industry's focus on creativity could overshadow cybersecurity's significance. There's also a tendency to view cybersecurity more as an expense than a vital investment. Furthermore, the intricate nature of cybersecurity and a dearth of internal expertise might contribute to this reluctance.

This oversight could lead to data breaches, legal issues, and tarnished reputations. Hence, it's imperative for MIS leaders to acknowledge the criticality of cybersecurity and integrate it into their core business strategy.

Recommendations for media & information services companies

Every company is different, and within the media and information services industry, business models can vary widely. Nevertheless, based on our findings from this study and our experience in hardening the defenses of MIS firms, these are some key points CISOs and CROs need to be sure they address when it comes to securing their enterprises against cyber risks.

1 **Align security with corporate strategy.** In the fast-paced world of media and information services, where content is king, it's crucial to align security measures with the overarching business strategy. For instance, streaming platforms like Netflix and Disney+ house vast libraries of proprietary content. A breach could lead to unauthorized leaks, impacting both revenue and brand reputation. Moreover, with the rise of digital-first content platforms like Spotify and Apple Music, ensuring the protection of intellectual property becomes paramount. MIS company platforms need security measures that not only prevent unauthorized access but also detect and respond to any breaches swiftly. By aligning security with business objectives, MIS companies can ensure that they protect their most valuable assets while also meeting the evolving demands of their audience.

2 **Prioritize security in all MIS operations.** The MIS industry is unique in its operational breadth, spanning content creation, post-production, distribution, and consumer engagement. Each stage presents its own set of cyber vulnerabilities. For instance, during content creation, scripts, raw footage, and other pre-release materials are highly sensitive. A leak at this stage, as witnessed with HBO's "Game of Thrones" episodes[6], can lead to significant financial and reputational damage. On the distribution front, platforms like Amazon Prime and Hulu must ensure that their user data, payment information, and viewing preferences are safeguarded. By embedding security at every operational level, MIS companies can ensure holistic protection, minimizing potential weak links in their security chain.

Recommendations for media & information services companies

3 **Foster CISO and CRO collaboration for content platform and cybersecurity strategy.** On the issue of collaboration, MIS industry executives could take a lesson from their counterparts in other industries. Only a quarter of MIS CISOs and CROs surveyed said they collaborated and coordinated across these two roles on a daily or several-times-a-week basis. By contrast, in other industries we surveyed, nearly a third (32%) of CISOs and CROs said they collaborated and coordinated daily or several times a week. In the MIS industry, where the lines between content and technology blur, the collaboration between CISOs and CROs becomes vital. By fostering regular collaboration between these two roles, MIS companies can ensure that both technological and content-related risks are addressed, leading to smoother launches and sustained audience engagement.

---

4 **Assess cyber risks in MIS mergers and acquisitions.** The MIS sector has witnessed a flurry of mergers and acquisitions in recent years, with giants like AT&T's acquisition (and later divestment) of Time Warner properties and Disney's purchase of 21st Century Fox. While these mergers offer vast opportunities for content synergies and market expansion, they also present significant cyber risks. Integrating different IT infrastructures, harmonizing data protection protocols, and ensuring compliance across diverse regulatory landscapes are challenges that must be addressed head-on. Before finalizing any merger or acquisition, MIS companies should conduct thorough cyber risk assessments, understanding potential vulnerabilities and formulating strategies to address them. This proactive approach can prevent potential breaches, safeguarding the combined entity's assets and reputation.

Recommendations for media & information services companies

5 **Take proactive measures.**

- Leverage data encryption for both stored and transmitted data to protect against opportunistic attackers.
- Implement principles of least privilege access, providing staff access only to network areas absolutely necessary for their roles.
- Strengthen authentication practices through multifactor authentication to deter hackers.
- Deploy and regularly update effective anti-malware applications to guard against a wide range of known and emerging threats.
- Maintain frequent, regular data backups to enable swift recovery from incidents like ransomware attacks.
- Provide systematic security training to staff, empowering them to identify threats and respond appropriately.
- Ensure comprehensive endpoint security, securing all devices interfacing with the network. Implement zero-trust principles to validate access rights before connections are established.
- Conduct regular penetration testing and apply security patches to stay ahead of attackers and ensure system integrity.

With some executive focus, the companies that tell the stories can avoid becoming the story

The media and information services sector faces a nuanced array of cybersecurity challenges amidst its digital evolution. As the narrative of creative content and next-gen platforms unfolds, the subplot of cyber threats thickens, demanding a robust defensive script. The insights from the cloud's horizon are promising, heralding enhanced security frameworks.

However, the real pivot lies in the boardrooms where decisions to intertwine cybersecurity within the business and operating models are made. A collaborative alliance between CISOs and CROs, comprehensive security measures spanning from content ideation and creation to distribution and consumption, and vigilant risk assessments in the saga of mergers and acquisitions are pivotal.

As the digital domain expands, it's imperative for the MIS sector to foster a cybersecurity culture that's as dynamic as the content it creates and the ways it creates it. By doing so, the sector not only safeguards its assets but also keeps its digital stage secure for the ongoing drama of innovation.

Notes

[1] Newzoo, “Last looks: The global games market in 2023” (May 16, 2024): newzoo.com/resources/blog/last-looks-the-global-games-market-in-2023

[2] Forbes.com, “The Gaming Industry: A Behemoth With Unprecedented Global Reach” (November 17, 2023): www.forbes.com/councils/forbesagencycouncil/2023/11/17/the-gaming-industry-a-behemoth-with-unprecedented-global-reach/

[3] Spiceworks, “Lessons from Netflix’s Password-Sharing Crackdown” (April 5, 2023): www.spiceworks.com/it-security/identity-access-management/guest-article/netflixs-password-sharing-crackdown/

[4] AP/U.S. News & World Report, “Netflix's Subscriber and Earnings Growth Gather More Momentum as Password-Sharing Crackdown Pays Off “ (July 18, 2024): www.usnews.com/news/business/articles/2024-07-18/netflixs-subscriber-and-earnings-growth-gather-more-momentum-as-password-sharing-crackdown-pays-off

[5] TCS Global Cloud Study, “Connected future: How cloud drives business innovation”: www.tcs.com/insights/global-studies/tcs-global-cloud-study

[6] The New York Times, “Hackers Threaten ‘Game of Thrones,’ as HBO Confirms Cyberattack” (July 31, 2017): www.nytimes.com/2017/07/31/business/media/hbo-hack-game-of-thrones.html

Executive champions

Akhilesh Tiwari
President — Communications, Media & Information Services Business Group, TCS

Ganesa Subramanian Vaikuntam
VP and Global Head — Cybersecurity Business Group, TCS

Contributors

Hatim Lokat
Global Head — Communications, Media & Information Services, Cybersecurity Business Group, TCS

Sujatha Gopal
Chief Technology Officer — Communications, Media & Information Services Business Group, TCS

For the most up-to-date content and news, download the 'TCS Perspectives' app for your iOS and Android device.

Download on the App Store

ANDROID APP ON Google play

Get more insights
If you would like to have more information on the TCS Risk & Cybersecurity Study, please visit on.tcs.com/risk-cybersecurity

For more information or any feedback, email the TCS Thought Leadership Institute at TL.Institute@tcs.com

About the Thought Leadership Institute

Since 2009, the TCS Thought Leadership Institute has initiated conversations by and for executives to advance the purpose-driven enterprise. Through primary research, we deliver forward-looking and practical insights around key business issues to help organizations achieve long-term, sustainable growth. For more information, visit **tcs.com/insights/global-studies**

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 56 years. Its consulting-led, cognitive powered, portfolio of business, technology and engineering services and solutions is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 601,000 of the world's best-trained consultants in 55 countries. The company generated consolidated revenues of US $29 billion in the fiscal year ended March 31, 2024, and is listed on the BSE and the NSE in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit **www.tcs.com**