CGRC™

Certified in Governance, Risk and Compliance

ISC2 Certification

Risk Management in Media and Entertainment

The media and entertainment sector covers many organizations, ranging from TV and film production companies to TV and radio broadcasters to newspaper, magazine, book and online publishers, among others. For these companies, content is key intellectual property. It can include finished products like music, videos and movies, but also material never intended to be public — scripts, contract negotiations, scenes that wind up on the cutting room floor and proposed content that's never produced.

The supply chain is a key source of risk because so many moving parts interact with each other. Key assets could be scattered across multiple companies worldwide as content is created, processed, edited and distributed. After nation-state malicious actors attacked Sony in 2014, proprietary content protection became the top priority for the industry. Pirated content affects the bottom line, and releasing confidential content can seriously impact brand reputation and artists.

Recognizing the challenges

Media and entertainment organizations could be exposed the increased cyber risks for these reasons:

Extensive remote work - Many if not most creatives work remotely in a highly collaborative manner and often from personal devices.

High-profile content - Content is a high-profile and attractive target to cybercriminals eager to monetize or accrue notoriety by leaking it.

Social media - It is critical for high-profile individuals to engage with fans and brands on social media to drive marketing campaigns. This exposes them to account hijacking, which could severely damage reputations.

Web-based assets - Digital assets such as streaming portals and ticketing sites proliferate in the sector, offering cybercriminals many more avenues of attack.

Media and entertainment organizations must account for superior customer experience. Digital innovations in the media and entertainment industry are focused heavily on customer experience with rapid consumer adoption of streaming services, online gaming and virtual reality. These services rely heavily on cloud-based services, IoT devices and mobile networks, and interruptions in service can degrade brand reputation.

Additionally, these organizations store the personal information of millions of people via relatively small transactions. They must demonstrate compliance with multiple regulations and standards without disrupting business processes and harming profitability.

Lastly, minimizing costs across the organization is an ongoing priority in media and entertainment. Many launches require large up-front investments before consumer sales result in profitability. Cybersecurity investments must be prioritized according to the organization's risk tolerance, but it is unwise to defer the investments necessary to protect content and customer data. The cybersecurity skills shortage exacerbates the challenges, making it difficult to fill certain roles. Hiring skilled cybersecurity professionals can also be quite expensive.

Toward effective risk management

As the media and entertainment continues to grow, piracy, extortion, disruption and the targeting of customers are likely to increase. The good news is that cyberattacks in this sector use tried-and-tested and more easily mitigated techniques, including phishing, credential stuffing and malware for vulnerability exploitation.

While media and entertainment companies have focused primarily on preventing pre-release content theft and monitoring post-release piracy, this approach's limitations are becoming increasingly apparent. Alongside focusing on prevention, they must also be able to detect and respond to security incidents by following a risk-based approach to cybersecurity.

A collaborative approach, where stakeholders in the digital value chain share information and pool resources while maintaining protection and vigilance through appropriate technology tools, can be the most cost-effective solution to deliver tangible security benefits for everyone involved.

How CGRC can help

Understanding, selecting and applying the proper framework falls within the responsibilities of a governance, risk and compliance professional. ISC2 Certified in Governance, Risk and Compliance (CGRC) demonstrates that you have the knowledge, skills and experience required for using various frameworks to manage risk and to authorize and maintain information systems.

Take the next step to a career in governance, risk and compliance with The Ultimate Guide to the CGRC. Find out how CGRC and ISC2 can help you discover your certification path, create your plan and acquire the knowledge and skills for a successful career.

Core risk management frameworks

- ☑ ISO/IEC 27005:2022
- ☑ NIST Risk Management Framework
- ☑ GDPR and other regional or national privacy regulations
- ☑ PCI DSS
- ☑ NIST Cybersecurity Framework