**Revolutionising Security Measures for Modern Content Consumption**

The landscape of content consumption has undergone a permanent shift. Traditional media formats and scheduled broadcasting have rapidly given way to the convenience, accessibility, and vast range of streaming services. Independent content creators now share the digital stage with established industry giants, and organisations across various sectors have embraced the mantra that "content is king." Online video has become a crucial tool for engaging with prospects and customers, offering limitless volumes of high-quality, personalised content at the click of a button.

To accommodate this new paradigm, the IT infrastructure of the industry is evolving at a rapid pace. Many organisations are prioritising Cloud transformation to expedite the delivery of exceptional content, optimising flexibility, scalability, and cost control. This transformation enables sophisticated streamlining, automation, and personalisation through technologies like AI, big data, and machine learning.

This era of limitless content and tailored experiences is an exciting time for both consumers and businesses. However, like any technological innovation, it has also attracted the attention of cybercriminals. These malicious actors actively seek security weaknesses in media organisations' IT infrastructure. Their actions can range from nuisance attacks, such as defacing webpages, to large-scale theft of intellectual property, with severe financial and reputational consequences for the victims.

As early as 2016, 28% of surveyed media organisations reported experiencing cyberattacks, and 38% reported loss of intellectual property. Many organisations also faced website disruptions during these incidents. Given the current geopolitical climate, successful cyberattacks have shifted from being a highly likely possibility to a near certainty that organisations must address.

**Being prepared for the worst**

Ransomware attacks pose a significant threat to media organisations, particularly those with multimillion-dollar film budgets. A pre-release leak alone can be damaging, as experienced by Netflix in 2021 when two highly anticipated films were leaked on pirate websites before their official launch dates. However, the consequences can be even more severe. Consider the 2014 cyberattack on Sony Pictures, where corporate data, including employees' personal information, scripts, plans for future films, and unreleased films, was leaked online. The attackers used wiper malware to erase the company's IT infrastructure. This attack was later attributed to cyberterrorists sponsored by a foreign government.

Media organisations must be prepared for worst-case scenarios like these. They need to secure their content and ensure swift and safe restoration of their IT infrastructure in the event of a successful attack, without resorting to paying ransoms to criminals.

**Developing media-ready cybersecurity**

In recent years, IT infrastructure has evolved to optimise the delivery of streaming services and on-demand content, with a significant increase in Cloud adoption rates. Moreover, media professionals, including freelancers, often connect from outside corporate infrastructure, relying on remote communication and collaboration. Consequently, the potential attack surface has expanded, particularly regarding access to valuable intellectual property, which hackers perceive as "low-hanging fruit."

In this context, a proactive approach to cybersecurity is essential. Organisations must continuously monitor the threat landscape and ideally seek support from technology partners with proven experience in securing media assets. Acting promptly on the latest intelligence is crucial.

Furthermore, as Cloud transformation accelerates, security ecosystems must be inherently Cloud-ready. Multi-Cloud and hybrid Cloud solutions provide advantages by adding an extra layer of resilience and facilitating integration with existing systems and processes that are not yet fully digitalised. These solutions open up opportunities for remote collaboration, even in post-production stages where teams are not necessarily located in the same place.

Regardless of the Cloud solution used, rapid restoration of IT infrastructure is vital in the event of a breach, ideally within hours rather than days. Air-gapped disaster recovery solutions, featuring immutable backups that cannot be accessed or modified until restoration is needed, prove ideal for this purpose. This ensures critical assets, such as unreleased content or viewers' personal data, remain secure and can be swiftly restored in the event of an attack, breaking the ransom payment model effectively.

**Cutting-edge cybersecurity tailored to media challenges**

Viewers' relationship with content is evolving, and creators and providers must strive to keep pace. While the opportunities are immense, the associated cybersecurity challenges must not be overlooked. Ensuring absolute content security throughout every phase of development while maintaining accessibility for viewers requires close collaboration between media organisations and their technology partners. It is an ongoing process, as cybercriminals continue to refine their tools and tactics.

If you wish to explore any of the subjects discussed in greater detail, feel free to contact us.