DATA-LOSS PREVENTION (DLP) FOR THE MPA CONTENT SECURITY PROGRAM

Contents:

The Challenge for MPA Partners

In 2009, the Motion Picture Association (MPA) and member companies released the first version of the MPA Content Security Program (CSP), a set of content security best practices intended to provide IT security assurances for MPA members. The program is intended to aid vendors and potential partners with data privacy and security, focused on data loss prevention (DLP) for proprietary media content. Producing agents in the motion picture industry that have relationships with MPA members need to implement security controls that meet the CSP requirements.

The MPA CSP compliance audits are conducted by The Trusted Partner Network (TPN) [TPN], which is owned and managed by the MPA. The audit process allows motion picture and television content owners to identify what standards are applied to each vendor based on the value and type of content handled. The TPN also facilitates the sharing of assessments with each of the motion picture and television content providers and owners.

The CSP includes references to multiple IT security frameworks and standards. To say that navigating standards such as NIST [NIST-CSF], ISO 27001 [ISO-27001], ISO 27002 [ISO-27002], CSA, ISACA [ISACA] , and SANS [SANS] can be difficult is an understatement. The fact is that many IT professionals will be overwhelmed by the amount and depth of IT security information contained in them. Multipoint Network helps vendors navigate the bumpy road from inception to audit and achieve MPA compliance by implementing security best-practices and industry leading products such as Endpoint Protector, which is designed to monitor, and protect your sensitive data with advanced cross platform data loss prevention. Trust Multipoint Network's experience and professional services to help your organization achieve MPA compliance. Our experience and services can help pave the pathway to a successful TPN audit.

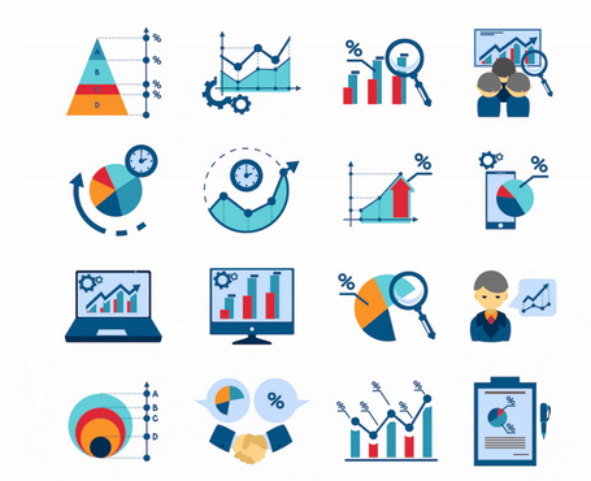
Importance of DLP to Media Content Security

Due to the increasing complexity of managing digital assets, cybersecurity has quickly become a major concern for companies that work with proprietary confidential data. The entertainment industry is a clear example. MPA Partners expect that their media content should be effectively protected using IT security DLP strategy. The fact is, cyber criminals are out there and they want to get inside your network, harm assets, and cost your company money. In 2014, Sony was subject to a data-breach that cost the company at least $15 million dollars with high estimates of over $100 million [SONY-REUTERS]. The fact that it wasn't the first time Sony had been breached is testament to the need for continuous attention to and improvement of IT security controls [SONY-TC]. The MPA Content Security Program's goal is to strengthen protections for content and associated data during the production, post-production, marketing and distribution stages of production.

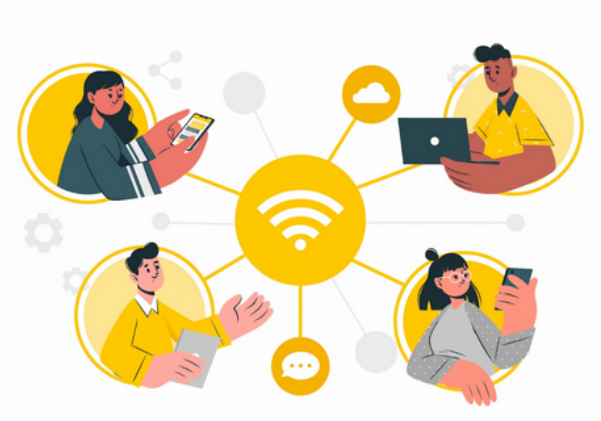
The specific goals of MPA CSP include:

Secure member content with effective IT security best practices

Protect member content from theft and accidental loss



Monitor and evaluate the content security implemented by third-party partners



Strengthen communication regarding security between members and their partners

Case Study: Level Up Meets CSP Compliance

Smaller media companies engaged with MPA Members may initially feel overwhelmed when trying to organize themselves to approach a CSP audit. We know this from experience. Recently, Multipoint Network helped LevelUp AV achieve MPA CSP compliance and implement an IT security program that ensures continuous compliance.

LevelUp AV consists of 25 employees and produces high quality movie trailers for upcoming films. Their IT infrastructure consists of a wireless office network that includes guest WiFi access, and a wired internal network. The wired internal network implements network security including firewall, and VLANS segment network devices that handle protected content. The media production network connects Avid Composer workstations to a shared storage RAID solution Authorization Network (for Avid air-gapped).

Our security product of choice is Endpoint Protector since it allows us to secure networks and endpoints cross-platform. LevelUp AV's network includes both Mac and Windows workstations and servers, so the need for an effective cross platform security product is critical.

Multipoint Network implemented a plan for the entire organization, its workflow and security controls for the protocols and operational procedures that meet MPA auditing standards. Our services also extend beyond planning security controls to include continuous monitoring of network and endpoint security.

Conclusion

Working with MPA partners requires CSP compliance. It's up to MPA vendors to protect the media content within their network, and implement DLP security controls. Multipoint Network can help guide your business through the process by helping you install and configure security best practices with a security product such as Endpoint Protector. Endpoint Protector is ideal for most media production companies because it offers enterprise level security protection, and is cross platform, extending protection to Windows, MacOs, and Linux endpoints and infrastructure. Multipoint Network is ready to provide MPA vendors with guidance, security design, and installation of security controls to meet CSP compliance.

References

[MPA-CSP] MPA Content Security Program
https://www.motionpictures.org/wp-content/uploads/2022/02/MPA-Best-Practices-Common-Guidelines-V4.10-FINAL.pdf

[SONY-TC] TechCrunch - Employee Data Breach The Worst Part Of Sony Hack
https://techcrunch.com/2014/12/16/hack-sony-twice-shame-on-sony/

[SONY-REUTERS] Reuters - Cyber attack could cost Sony studio as much as $100 million
https://www.reuters.com/article/us-sony-cybersecurity-costs-idINKBN0JN2L020141209

[NIST-CSF] NIST Framework for Improving Critical Infrastructure Cybersecurity
https://www.nist.gov/cyberframework

[ISO-27001] ISO 27001 - Information security management
https://www.iso.org/isoiec-27001-information-security.html

[ISO-27002] ISO 27002 - Information technology — Security techniques — Code of practice for information security controls
https://www.iso.org/standard/54533.html

[ISACA] ISACA - COBIT Focus Area: Information & Technology Risk
https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ku2gEAC

[SANS] SANS - Cyber Security Training, Certifications, Degrees and Resources
https://www.sans.org/

[TPN] Trusted Partner Network
https://www.ttpn.org/

Images:

Open lock vector created by pch.vector - www.freepik.com
Employee engagement vector created by pch.vector - www.freepik.com
Cloud security vector created by vectorjuice - www.freepik.com
Data collection vector created by macrovector_official - www.freepik.com