Security Trends in Media &Entertainment

Why Traditional Information Security Doesn’t Fit Media & Entertainment

Marc Zorn (CISSP, GIAC, CISA)
eZorn Consulting Group

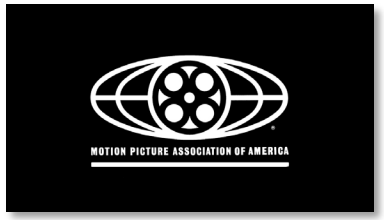
Transition Issues from Film Security

- Film security was based primarily on physical measures
- Film was basically processed "daily" and scanned to Digital Intermediates (DI)
- "Post-Production" began after photography
- FX mostly were "practical" or done in Post
- Threats were primarily from Post onward
- **Threats to DI / digital media looked like IT Security**

ISO 17799 / 27000 domains

- Security policy
- Security Organization
- Asset Management
- HR Security
- Physical and Environmental
- Comm and Ops Management
- Access Control
- Systems Admin
- Incident Management
- Compliance

MPAA Adapted ISO 27000 to Create Industry "Best Practices"



- Began the Security Audit Program
- Kept existing highly-political process
- Sponsored by member studios (DFPSWU)
- Non-member studios intentionally excluded
- Focused on Post-Production vendors
- Protection of IP primarily sound & picture
- Primarily physical and infrastructure controls

MPAA Audit Drawbacks

- Largely missed workflows and changing digital technologies
- Every studio performed their own audits
- Unreasonable focus on surveillance and "obstructive" controls
- Preoccupied with screeners and Internet piracy
- Risks always changing
- Based on Compliance

  and **NOT RISK**

MOTION PICTURE ASSOCIATION OF AMERICA

A Word about Production Culture

A Word about Production Culture

Production Culture

- Unique technologies and workflows
- Fundamentally different from corporate
- Highly-trained and highly-competent technologists
- Security is not a priority, but is a concern
- Often asked to devote some of our creative budgets to security
- No time to talk at “Production Speed”

Contiguous Workflow and Polymedia

- Workflows now digital from Dev to Distro
- IP is created now along entire arc
- Blurs the distinctions between phases
- Collaboration begins at development
- Traditional roles are changing
- Technologies popping up to support contiguous and bi-directional workflows

Incremental Changes in Production Security

- Digital Asset Management (DAM) in some form is part of entire process
- Identity Access Management (IAM) new requirement
- Digital Certificates and Federated ID enable access
- Cloud technologies employed primarily thru object storage or task processing, but soon beginning to end
- "Production Speed" now starts at the beginning
- We are obviously diverging from traditional Infosec

Moving Away from Infrastructure

Local	Shared	Distributed	Cloud
Weak Identity Credentials			Strong Identity Credentials
Direct Control	Shared Control	Delegated Control	federated Control
Dedicated Access	Local Area Network	Wide Area Network	Internet Access
Clear text			Strong Encryption

Innovation of Production Technologies

- Interoperable Mastering Format (IMF)
- SMPTE ST-2110 ST-2059, and others
- Academy Color Enhancement System (ACES) workflows
- Tool suites integrate shooting logistics, camera functions, color calibration

- ***Lost Lederhosen***

The Rise of Metadata Foretold !

- Metadata is no longer incidental or a luxury
- Soon will be part of every workflow
- Metadata used for everything from documentation, to authorization, instructions, logistics, credits, trivia, marketing, copyrights, contract terms, royalties, codec, photo data, forensic info, to archive

Implications of Metadata Management

- Metadata is now Intellectual Property
- Safeguards and controls must become part of every workflow and stored data
- Security won't continue to be just about compliance or risk
- Now ***enabling*** technology and an integral aspect of everything

Improvement Opportunities

- Demand security built into all tools, networks, storage, collaborations spaces
- Creative budgets include improved (secure) tools
- Don't use any tool that is not proven to be secure
- Do not rely on someone else to manage security for your data (especially cloud)

Push **HARD** on all technology providers for integrated security

- Cloud tool do not equate to safety
- Manage Metadata (because it's IP, too)
- Demand Identity Access Management, perhaps using digital certificates
- Demand encryption of ALL data at rest and in transit
- Don't use tools unless they can demonstrate that it is secure

Summary

- Current Infosec policies and "Best Practices" are obsolete
- Continued focus on infrastructure controls is almost unimportant
- We are now in collaborative space
- Storage location of encoded data will be irrelevant because data must protect itself
- Security is enabling innovation and no longer somebody else's problem