Security Holes and How to Fill Them

HPA Tech Retreat, 23rd February 2017

Laurence Claydon – CTO, Motion Picture Solutions Ltd

Introduction

- History of Content Piracy
- The Role of Physical Media in current Content Protection Practice
- File-Based Workflows
- Concepts - Environmental Security and Content Security
- Balance of Speed vs. Security
- Identifying the Security Holes – Risk Profiling
    - Content Risk Classification Example
    - Factors that increase risk – Localisation and Day-and-Date
    - Workflow Risk Profiling
- Filling the Security Holes
    - Risk and Mitigation
    - Application of Encryption at Rest
- Conclusions

What's not covered…

- Firewall Whitelisting, Network Security and ACLs
- Intrusion Detection and Prevention
- Emerging encryption standards (e.g. Elliptic Curve Cryptography)
- Forensic Watermarking Technologies
- FIPS compliance
- ISO27001
- The obvious benefits of multi-factor authentication
- The threat of Quantum Computing technology to reverse every prime-number-pair algorithm in a few years time…
- Anything that might introduce Fear, Uncertainty and Doubt….

Aim of this Session

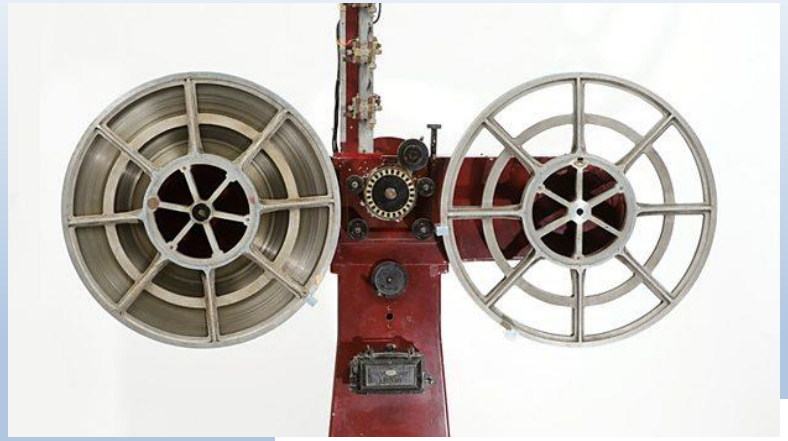
- Explore Content Security Principles that:
  - Provide fundamental rules that allow anyone to handle content securely
  - Provide fundamental rules for workflow, content transfer and even facility design
  - Outline Risk, and how to Mitigate Risk
  - Can be used to build into any workflow – Production, Post Production and Distribution
  - Provide a basis for further discussion and industry initiatives
  - Are clear and easy to understand

History of Content Piracy

- *Miserere* by Gregorio Allegri
  - Composed during the reign of Pope Urban VIII c.1630
  - Performed in the Sistine Chapel in the Vatican
  - Closely-guarded - handed down to succeeding Choir Masters under strict supervision
  - Transcription was forbidden, punishable by ex-communication
  - Remained exclusively within the Vatican for over 100 years...
- 1770
  - Wolfgang Amadeus Mozart, aged 14 visits Rome
  - Hears *Miserere* twice, and transcribes it from memory
  - Following a meeting with Charles Burney, it is published in London in 1771

History of Content Piracy

- Advance of Technology increases Risk of Piracy



Early attempts to combat Piracy

- Tell people not to do it….

Physical Media – Recent History

- Content Protection is often based upon physical security measures
  - Physical Media in regular use as recently as 2011/2012
    - Professional Videotape - e.g. HDCAM SR
    - Data tape e.g. LTO tape
    - 35mm Film Interpositives
  - Physical security - easier to control risk
    - Copy controls/number of copies
    - Restrict playback with professional standards (e.g. HDCAM SR, 35mm Film)
    - Physical security methods, (locks, safes, barcoding/asset tracking)
    - Hand carries for high-risk content (Sound Masters, Interpositives, Image data on LTO)
- No surprise that most industry security standards are based up on access restriction and controls to physical media

What's changed in the last 5 years?

- 2011 – a turning point
  - Japan Tsunami - HDCAM SR tape stock production interrupted for 5 Months in 2011
    - Rapid adoption of File-Based workflows
    - Rapid uptake of Electronic File Transfer Toolsets
  - File-based delivery overtakes physical delivery
    - 2010 – most DCDM/DPX data for D-Cinema Mastering and Film Recording was delivered on LTO3/4
    - 2012 – most source data received electronically via 10Gb/sec fibre
    - Bandwidth cost/speed/availability improves
    - Improvements to secure file acceleration tools to handle content types natively (e.g. no need to TAR-up 2TB DPXs)

Electronic File Delivery

- Benefits are Clear
  - Efficient – no need to copy out, ship and then load data from physical media
  - Benefits day-and-date localisation
  - Encryption in Transit and at Rest
- Security Risks
  - Transfer server storage often lives in DMZ (internet facing)
  - Content may be copied/sent one-to-many
  - Greater controls required
    - IP/recipient whitelisting
    - Password Distribution
    - Account Expiry Management
    - Download link expiry/one-time only downloads
    - Remove data from DMZ storage as fast as possible
  - Security based upon passwords – credentials are regularly SHARED

Environmental Security

- Physical Measures
  - Locks, Access Controls
  - CCTV
  - Perimeter Fences, Walls, Bars
  - Security Guards, Dogs
  - Staff background checks, searches
- Digital Security
  - Firewalls, Intrusion Prevention and Detection
  - Network Segregation
  - Role-Based Access Control (RBAC)
  - Endpoint Protection
  - SIEM Systems/Log Monitoring

- Management and Policy
  - Security Organisation
  - Staff Training
  - Confidentiality Agreements
  - Segregation of Duties
  - Staff background checks, searches
  - Account Management
  - Wireless Policy and BYOD
  - BYOD
  - Content Tracking
  - Content Transfer Systems

Environmental vs. Content Security

- Environmental Security
  - Assumes content is protected in a NON-HOSTILE ENVIRONMENT
  - Secure the Environment and the Content will be Secure
  - Frameworks are necessarily complex – Uniformity of adoption is challenging
  - Many variables = Complexity = Risk
  - Many environments add exponential factor to Risk
- Content Security
  - Assumes content exists in a HOSTILE ENVIRONMENT (e.g. DCI)
  - Protection therefore needs to be provided to the content itself

Balance of Speed vs. Security

- Day and Date Theatrical Release
  - Day-and-Date is itself an Anti-Piracy measure
  - Production delivering into localisation and distribution facilities with tighter deadlines
  - Projects often shared across multiple facilities
  - Tight deadlines lead to cut corners increasing risk
- Late Delivery = Loss of Box Office and Revenue
- Theft/Loss of Content = Loss of Box Office and Revenue
- Speed and Security are equally important

Identifying the Holes – Identifying Risk

- Content Risk Parameters
  - Size – is it small/easy to lose or steal?
    - 4GB Quicktime – High Risk
    - 12TB 4K DCDM – Lower Risk
  - Content Type – is the content complete, or an element?
    - Textless Section – Lower Risk (depending upon content)
    - Complete proxy-res Quicktime with Sound and Image in Sync – Very High Risk.
  - Time
    - Pre-Release – Highest Risk
    - On General Release – High Risk
    - Post Release/Archive – Lower Risk

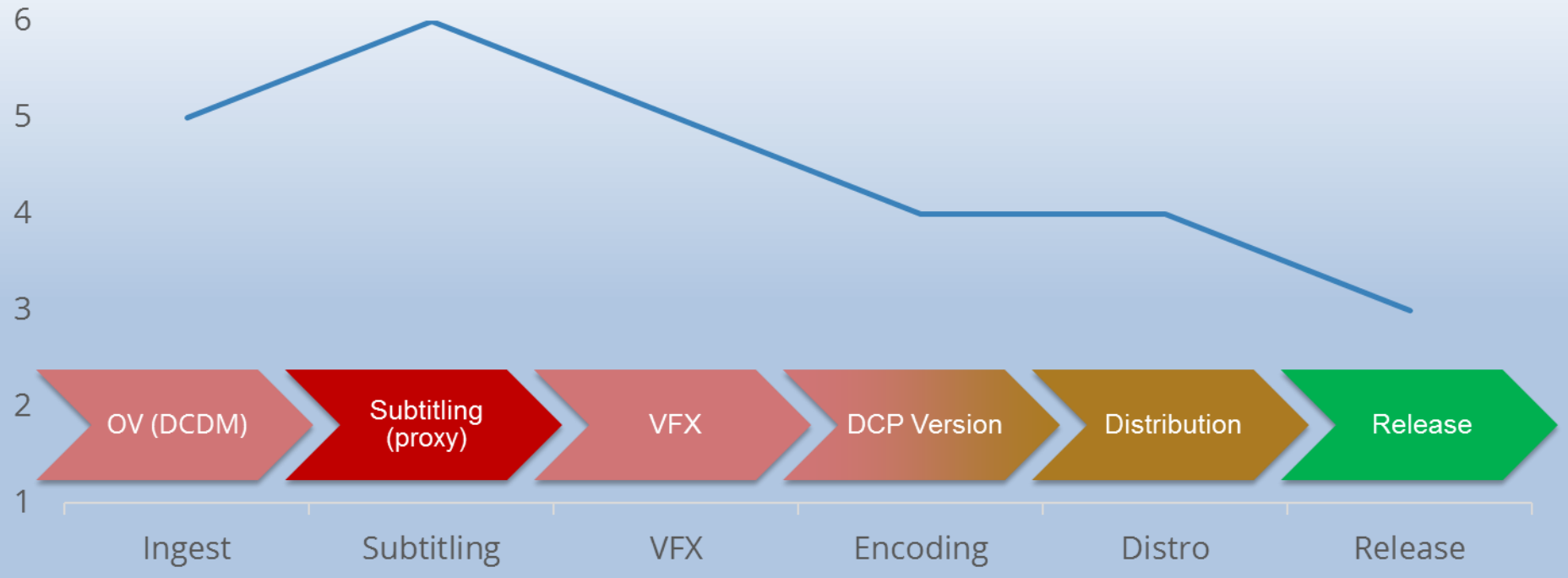
Making it Easy

- Requirements
  - Producers/Data Wranglers can track risk upon receipt
  - Straightforward and Easy to Remember
  - Know exactly how to categorise each type of content
  - Make recommendations to client where necessary

Content Security Risk Classification - Example

1. Archive Content
2. Back Catalogue, Encrypted
3. Post Release, Encrypted DCP
4. Pre-Release, Encrypted DCP
5. Pre-Release, e.g. DCDM/DPX Images, Unencrypted, Incomplete
6. Pre-Release Screener, Unencrypted, Complete

Theatrical Localisation Workflow - Example



Risk Parameters in Localisation

- Size – is it small/easy to lose or steal?
- Content Type – is the content complete, or an element?
- Time – Pre Release/Post Release/Archive
- Availability – Original Version Workflow
    - Production, Editorial, Dailies
    - VFX
    - Digital Intermediate
    - Sound Dubbing
    - Digital Cinema
    - Broadcast Deliverables

Risk Parameters in Localisation

- Availability – Foreign Language Localisation Workflow
    - Sound Dubbing Facilities – FRIGS, Latin American Spanish, Canadian French etc…
    - Subtitle Translators
    - Subtitle Finishing
    - Digital Cinema
    - Broadcast Deliverables
- Versioning requires ~50+ Language Versions
- 100+ pre-release copies of the content sent/streamed electronically
- Subtitle files still commonly sent via email…

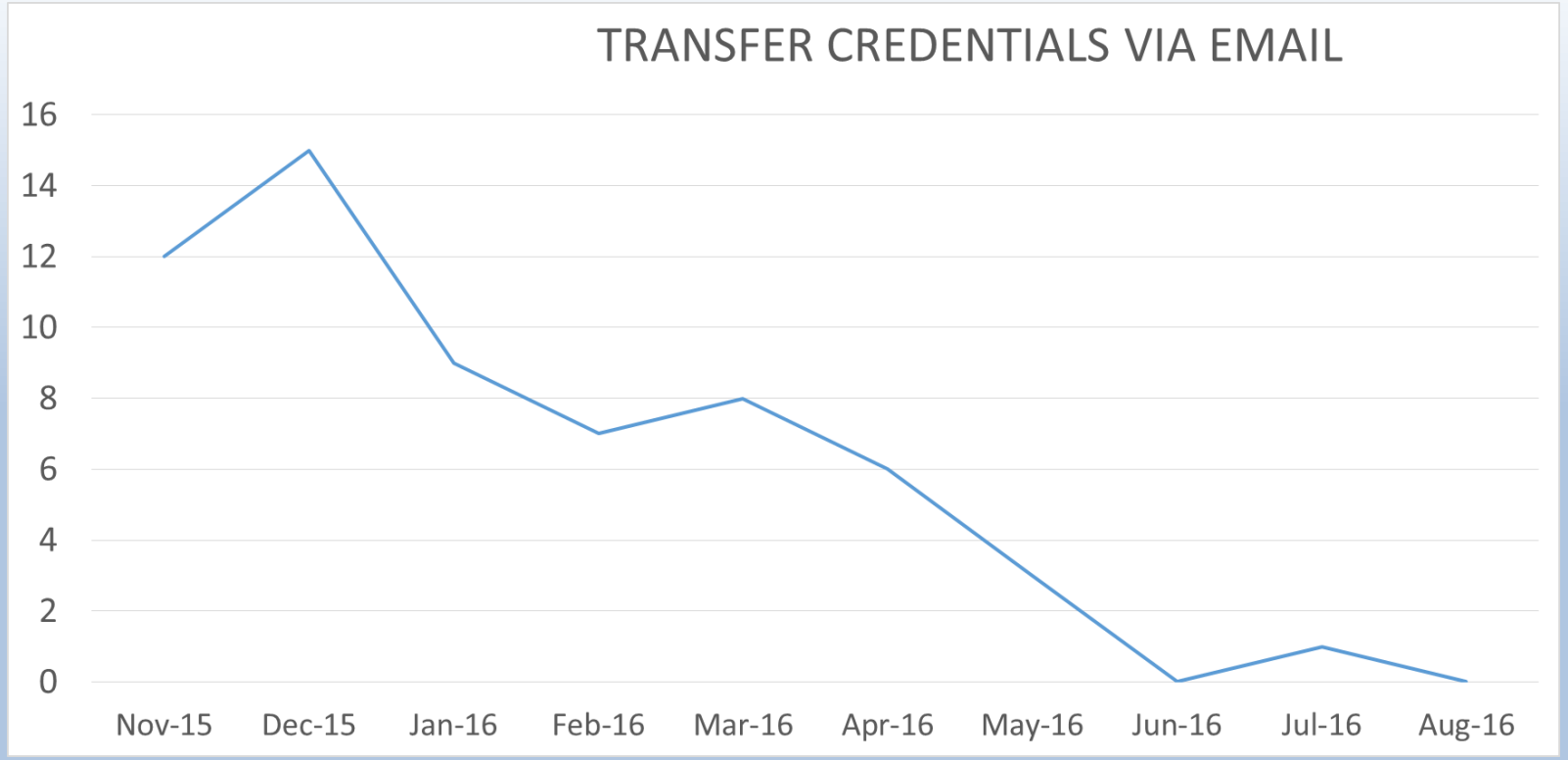
Risks in Content Data Transfer

- Pros - Encryption in Transit, Encryption at Rest, FIPS 140-2 Level 3 Security
- Downside - CREDENTIAL SHARING
  - Content Transfer Notifications mostly sent via Email
  - Contain the URL or LINK
  - Contain the USERNAME
  - Contain the PASSWORD
  - Cc'd to many, Forwarded, Replied to etc…
- Email usage policies prohibit the *sharing of Passwords by Electronic Means…*
- …Proving that Policies rarely get read…
- Who's doing it? – EVERYONE!

Dealing with the Issue…

- Classified as a Security Incident – Escalate Immediately
- Contact all Parties to :-
  - Notify of Incident
  - Explanation as to why this is a RISK
  - Request for Password Change
  - Request that the new Password is communicated Out-Of-Band (e.g. Privnote)
  - Back to Business

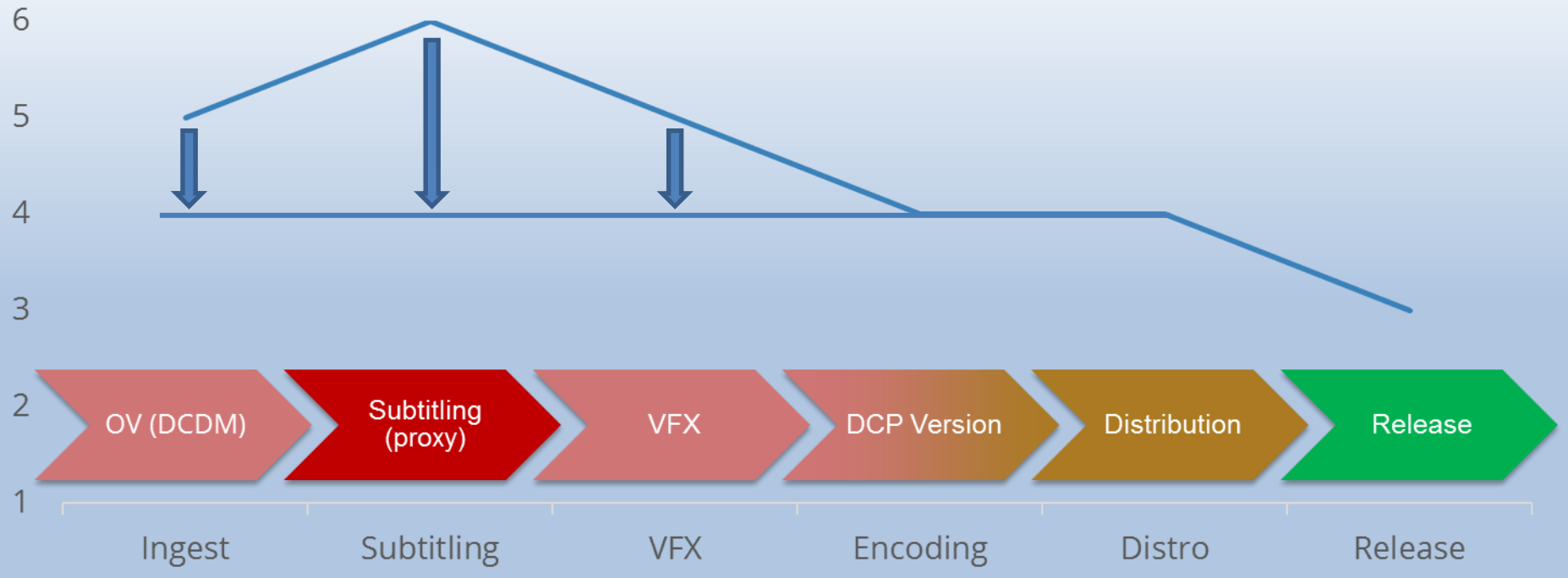
Security Incident Reduction Initiative



Further Risk Mitigation – PREVENTATIVE

- Encryption-at-Rest
- Requirements for Efficient Workflow
  - 128-bit (minimum) or 256-bit (preferable) AES Encryption
  - Media Agnostic
  - Operating System Agnostic
  - Application Agnostic
  - Secure Key Management
  - FIPS or NIST traceable
- Toolsets now exist / in-development

Theatrical Localisation Workflow - Example



Further Considerations

- Risk Profiling can also define…
  - Network Segregation
  - Infrastructure and Storage
  - Facility Layout and Physical Access Control
  - Role Based Access Control
  - Segregation of Duties
  - Content Transfer
  - Security Policy and Procedures
  - Environmental Security!

Conclusions

- Environmental Security is Complex and Variable
- Multiple Content Data Transfers Increases Risk (e.g. Localisation)
- Risk Profiling Affords Secure Content Handling
- Encryption at Rest Mitigates Risk
- Security Design for all areas can be driven by Risk Profiling

And…

- Don’t send passwords via Email…

Thank you

Laurence Claydon – CTO, Motion Picture Solutions Ltd