

2010 Annual Trending Report
Motion Picture Association of America, Inc.
Site Security Program

Contents

2	Executive Summary
4	The Average Vendor
5	Site Survey Trends
5	Post-Production
10	Audio, Dubbing, and Sub-Titling
14	Replication

Appendix

I	Geographic View of Vendor Locations
II	MPAA Content Security Model
III	2010 Best Practices Overview

Executive Summary

Over the past three years, the MPAA Site Security Program has performed surveys of over 300 vendor locations utilized by MPAA Members worldwide. In 2010, the program transitioned from using a maturity model to a series of 10 best practices, issued by the MPAA in February 2010. Best practices are based on the maturity model but tailored for different facility types. They are intended to provide current and future vendors utilized by MPAA Members with an understanding of general content security expectations and current industry best practices. In addition, best practices are used as a basis for the site surveys. In 2010, site survey reports provided a comparison between site security and their respective best practices – the trending report summarizes performance for sites visited, including for the first time at the most detailed element level.

During the past three years, we have also seen significant changes across the industry. The industry continues to move from a tape based to digital workflow, and new vendor services (such as digital cinema and 2D to 3D conversion) are now mainstream and a permanent fixture in the value chain. As we look towards the next year, we will continue to find a continued push for digital distribution, and the shortening of content windows will pose additional risk to the industry, as vendors will need content sooner to perform functions, such as encoding/transcoding and authoring.

The Average Vendor

The average vendor surveyed is difficult to define, as sites operate in different stages of the content's life cycle with differing workflows — post-production, DVD manufacturing, digital and physical distribution, and creative advertising, among others. In 2010, over 100 reports were issued for vendors in 24 countries. An increasing amount of sites requested are international – 48% of vendors surveyed were located outside of the United States compared to 33% in 2009.

General Trends:

- The areas of control environment have seen an increase in security related to the formal development of policies and procedures, but need to improve upon the performance of risk assessments focusing on loss prevention, as well as background checks on individuals handling content.
- Sites performed well in areas where physical security is incorporated as a necessity to their particular workflow – e.g., shipping and receiving.
- Other areas of physical security related to security processes – such as inventory counts and the periodic review of keycard access rights, continue to need improvement.
- There is generally less maturity when it comes to

digital security. This may be due to several factors. Best practices may be more difficult to attain and require significant capital investment. Tools and software used must be available, cost effective, and mature to match workflow constraints. In addition, smaller vendors may have less IT expertise in-house, which may lead to them underestimating digital-related risks.

- Sites typically need improvement when creating an ongoing process around security installations implemented, whether physical or digital, by defining monitoring and detective controls.

Site Survey Observations

The three most common facility types surveyed were Post-Production; Audio, Dubbing and Sub-Titling; and Replication. Trends have been included for each of these categories and highlighted as follows:

Post-Production — There were 39 large and small post-production sites visited in 2010. Post-production vendors consisted of traditional vendors, focusing on a combination of editing, audio, duplication, and versioning services, as well as emerging vendors, focusing on digital cinema mastering/replication and 2D to 3D conversion. Post-production vendors are handling high-resolution, pre-theatrical content that is generally unencrypted. Both physical and digital risks must be accounted for equally.

- Generally, vendors have developed policies and procedures that met or exceeded best practice, but, on average, did not meet best practices set for organizational security measures, including criminal background checks and establishing adequate incident response plans.
- Post-production vendors fare well in the areas of protecting and tracking assets, but require improvement assessing inventory compared against system records.
- Sites surveyed met best practices related to logical production access – which is dictated by unique users to gain access to content storage. However, vendors overall are having difficulty meeting Internet and end-user computing restrictions.
- When compared to all post-production sites, the digital cinema mastering and replication houses that were surveyed appeared to be consistently stronger in security across the control environment, physical security, and digital security areas. However, digital cinema sites surveyed were mainly made up of the two largest post-production vendors, and all but one facility surveyed was part of existing and ongoing operations at that location. As such, this may not be representative of all digital cinema vendors.

Audio, Dubbing, and Sub-Titling — There were 11 audio, dubbing, and sub-titling sites surveyed in 2010. Audio, dubbing, and sub-titling may be viewed as having less risk, as generally only audio is handled. However, sites many times handle pre-theatrical picture content as well, whether performing audio layback or dubbing. Physical security perhaps has more relevance due to the nature of the working environments. Audio facilities have among the most relaxed company cultures of the facilities surveyed and often times consist of specialists with years of experience, operating independently of the larger post-production companies. In general, elements produced on-site have limited digital tracking and are shared with clients using standard unencrypted channels (e.g., FTP). Such vendors may view this as acceptable practice given the perceived lower level of value associated with audio clips, as compared with high-resolution video.

Replication — There were 19 replication sites surveyed in 2010, mostly outside of the United States. Replication risks center around loss prevention – even a single DVD removed from the facility can cause a high definition image to appear on the Internet. Limiting employee exit points, a strong exit search process, and securing emergency exits are paramount for replication houses. Replication sites varied from best-in-class security, highlighted by sophisticated body scanners used in an exit search process, to international vendors with limited exit search process, limited resources for loss prevention, and poor controls related to scrapping of discs earmarked for disposal.

Program Impact

Although it is difficult to directly compare site results over the past three years, there have been improvements made across the control environment, physical security, and digital security:

- Control Environment: Over the past three years, we have seen a greater push towards creating central security functions, many that oversee both digital and physical security functions. Organizational security has improved through the introduction of formal programs, such as training initiatives.
- Physical Security: Physical security improvements can be attributed to best practices, which allow vendors to plan for security in facility design, and also understand general expectation levels that were not previously available.
- Digital Security: We are seeing a greater emphasis on security around infrastructure, storage systems, and transfer tools. Slowly the message is getting out that all content transferred needs to go over encrypted channels.

Overall, best practices have been adopted across the industry and praised as a good foundation for discussions between vendors and content owners.

The Average Vendor

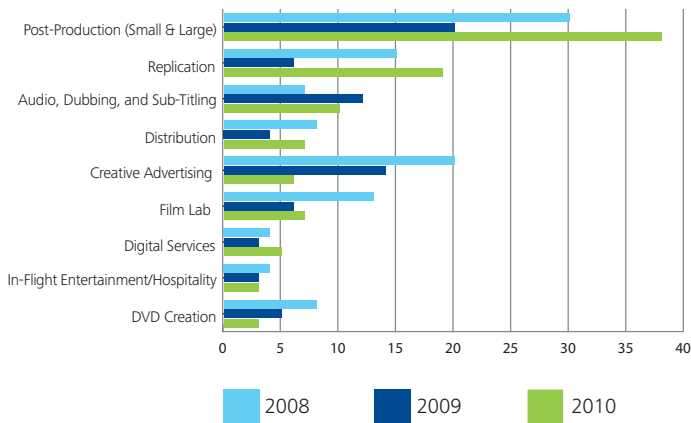
Vendor Makeup

In 2010, Deloitte & Touche LLP (Deloitte & Touche) surveyed 95 vendor sitesⁱ (75 new) representing a diverse mix of facility types and regional locations, spanning the entirety of the post-production lifecycle. Post-production (large and small), replication, and audio, dubbing, and sub-titling vendors were the most frequently requested facility types. Other facility types, such as creative advertising and transport vendors, significantly decreased as compared with historical levels.ⁱⁱ

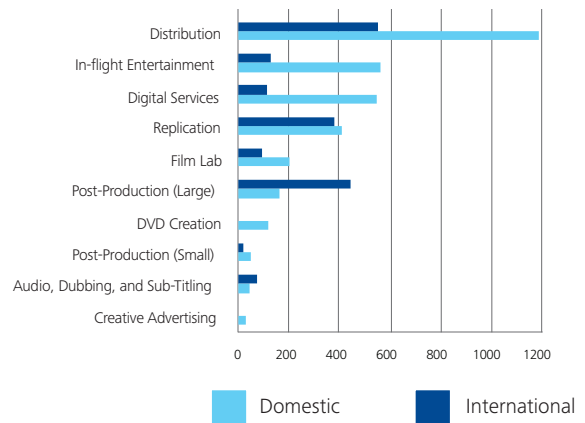
Describing the average vendor and the trends common to all facility types continues to be difficult, as each site features varying numbers of employees, facility sizes, and funds budgeted for security purposes. Evidenced by the 10 best practice guides published by the MPAA in February 2010, each vendor features a unique risk profile in terms of content handled and operates using a variety of distinctive workflows and business models. Adding to the complexity are new and emerging vendor facilities that were visited this year, including digital cinema mastering/replication and 2D to 3D conversion vendors.

While the majority of this year's surveys were conducted in the United States (52%), the program is seeing increased survey requests in global locations, with 24 countries visited in 2010. Please refer to Appendix I for a geographic display of states and countries where vendors were surveyed since 2007.

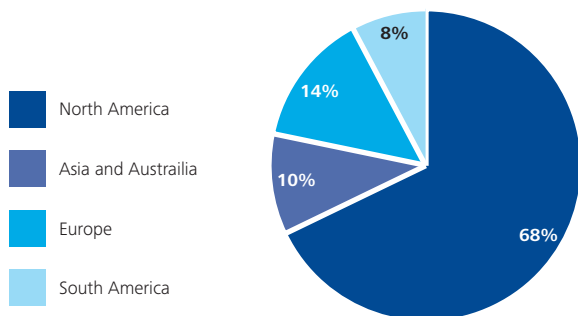
Facility Types Surveyedⁱⁱ



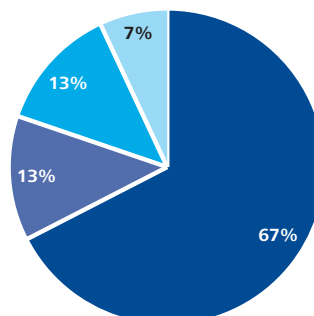
Average Employees by Facility Type



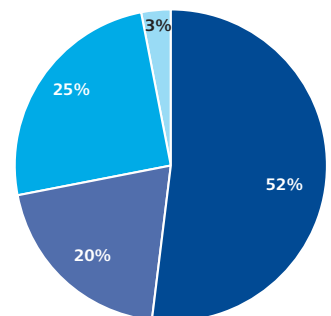
Breakdown of Sites Surveyed by Continent in 2008



Breakdown of Sites Surveyed by Continent in 2009



Breakdown of Sites Surveyed by Continent in 2010



Site Survey Trends: Post-Production

Similar to past years, post-production vendors constituted the majority of sites surveyed in 2010. Post-production vendors consisted of traditional vendors, focusing on a combination of editing, audio, duplication, and versioning services, as well as emerging vendors, focusing on digital cinema mastering/replication and 2D to 3D conversion.


Post-production companies are generally handling clean, high-resolution content well in advance of the theatrical release. The risk profile of a post-production site needs to take into consideration both physical and digital leaks, as sites will handle both physical and digital elements. Although overall workflows have been moving increasingly to digital in the past year, physical tapes continue to be common. Inventory tracking systems need to be in place, and controls around inventory management (e.g., inventory counts) needs to be improved. Digitally, file sizes and network throughput perhaps poses the greatest challenges.


File sizes dictate how content can be worked on, stored, and the security levels - generally stored files are unencrypted. Conversely, throughput is a key factor in determining whether it is economical to send content electronically or by physical means.


Site Characteristics


Sites Surveyed:	Large – 17 Small – 22
Avg. Employees/Temps:	Large – 246 Small – 37
Geographic Concentration:	64% Domestic 36% International

Control Environment		Physical Security			Digital Security		
Organization Maturity	Competency	Facility	Asset Management	Transport	Infrastructure	Content Management	Content Transfer
Organization Maturity	Recruitment & Personnel	Facility Access	Inventory & Asset Management	Shipping & Receiving	Infrastructure Security	Content Authorization	Transfer Security
Policies & Procedures	Training & Education	Facility Security	Physical Asset Security	Packaging & Transport	System Security	Content Tracking	Transfer Authorization
Incident Response	Vendor Management	Facility Authorization			Infrastructure Authorization		Transfer Tracking
Process Management		Facility Monitoring			Infrastructure Monitoring		

 On average, over 75% of vendors met best practice levels

 On average, 50 - 75% of vendors met best practice levels

 On average, 25 - 50% of vendors met best practice levels

 On average, less than 25% of vendors met best practice levels

Post-Production (cont.)

In addition to comparing performance to best practice levels, we also assessed post-production vendor performance in large vs. small vendors, and digital cinema sites vs. all post-production. We continue to look at the size of the facility to understand if there are differences in security levels based on employee size. In addition, digital cinema has been an emerging vendor type requested and poses unique risks related to mastering and key management.

Large vs. Small Vendors

Post-production vendors surveyed in 2010 were highly differentiated in terms of facility size and number of employees. On average, large post-production sites employed over 240 employees and temps, while small post-production sites averaged approximately 35 – excluding the two sites surveyed that perform Digital Cinema replication and distribution, small post-production sites employed only 19 employees on average.

Key Trends

- Large post-production vendors consistently averaged higher in Control Environment elements. It was observed that larger facilities typically had confidentiality agreements in place when compared with smaller facilities. This may be expected, as smaller sites have fewer personnel who interact directly with each other on a regular basis.
- Differences between large and small post-production facilities varied. Large sites, on average, had better security regarding electronic access and camera systems, while smaller sites on average had better security around alarms, master keys, and production systems. This may highlight that larger sites are more mature regarding the use of access control points, while small vendors may rely on keys to a greater extent. In addition, smaller facilities are more likely to be open only during business hours, while large sites are generally open 24x7. As such, alarms are of greater importance to small sites.
- Regarding digital security, larger post-production houses consistently performed better than small houses. This may be indicative of having in-house personnel dedicated to IT administration. Small houses may have more limited budgets allocated to technology and security tools, and may also outsource their IT function. Having an external IT support staff may pose an elevated risk to small post-production facilities.

Emerging Sites: Digital Cinema Mastering and Replication

In 2010, we also saw an increase in requests related to digital cinema sites, with eight of the 39 post-production sites surveyed. Generally, digital cinema mastering is performed at a centralized location, and copy masters are distributed to domestic and international sites that replicate content onto encrypted hard drives and distribute to exhibitors. Security at standalone replication sites may be viewed as less important, comparatively, as content is encrypted from the incoming copy master to replicated hard drives. Since content is not unencrypted and stored at replication sites, digital security is generally considered not applicable. Shipping and transport to digital cinema packages also becomes less of a concern.

Key Trends

- When compared to all post-production sites, the digital cinema mastering and replication houses that were surveyed in 2010 appeared to be consistently stronger in security across the control environment, physical security, and digital security areas.
- One cause may be that the eight sites that were surveyed consisted of the larger post-production companies. All but one facility surveyed was part of existing and ongoing operations at that location; for example, it is common for digital cinema replication sites to be a secured room in a film lab or print distribution site.

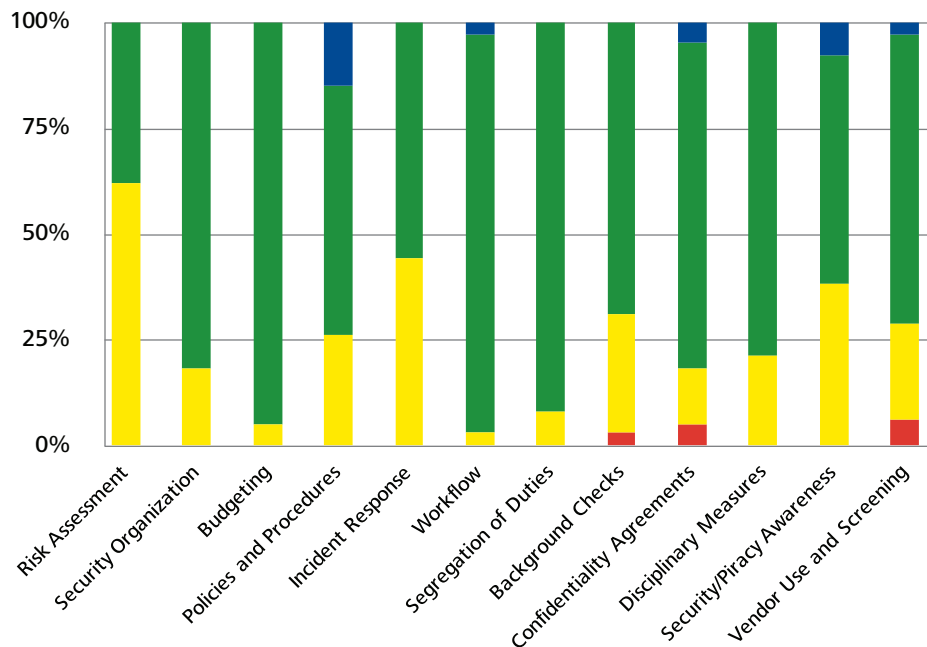
Post-Production (cont.)

Performance vs. Best Practices

The charts below are a graphical representation of the percentage of post-production vendors that have met best practices for each element across the three domains of control environment, physical security, and digital security.

Control Environment

Overall, control environment results highly varied for post-production vendors. Generally, vendors have developed policies and procedures that met or exceeded best practice, but, on average, did not meet best practices set for organizational security – for example, the majority of vendors did not perform formal risk assessments, and close to a third did not meet best practice for background checks. Risk assessments are important to the core of the vendor’s security management system function - risk assessments focus on improving security from within - through internal discussions of security in each stage of the workflow and by performing security self-assessments. Background checks suggest criminal background checks for employees handling content, unless restricted by local laws and regulations. Background checks help to give management comfort when individuals are required to handle content as part of their job function. In addition, the Incident Response dimension also had a high percentage of considerations; incident response looks to formally define an incident response process if any threats occurred. Vendor sites may lack formal incident response policies if security or threats in the past have not occurred.

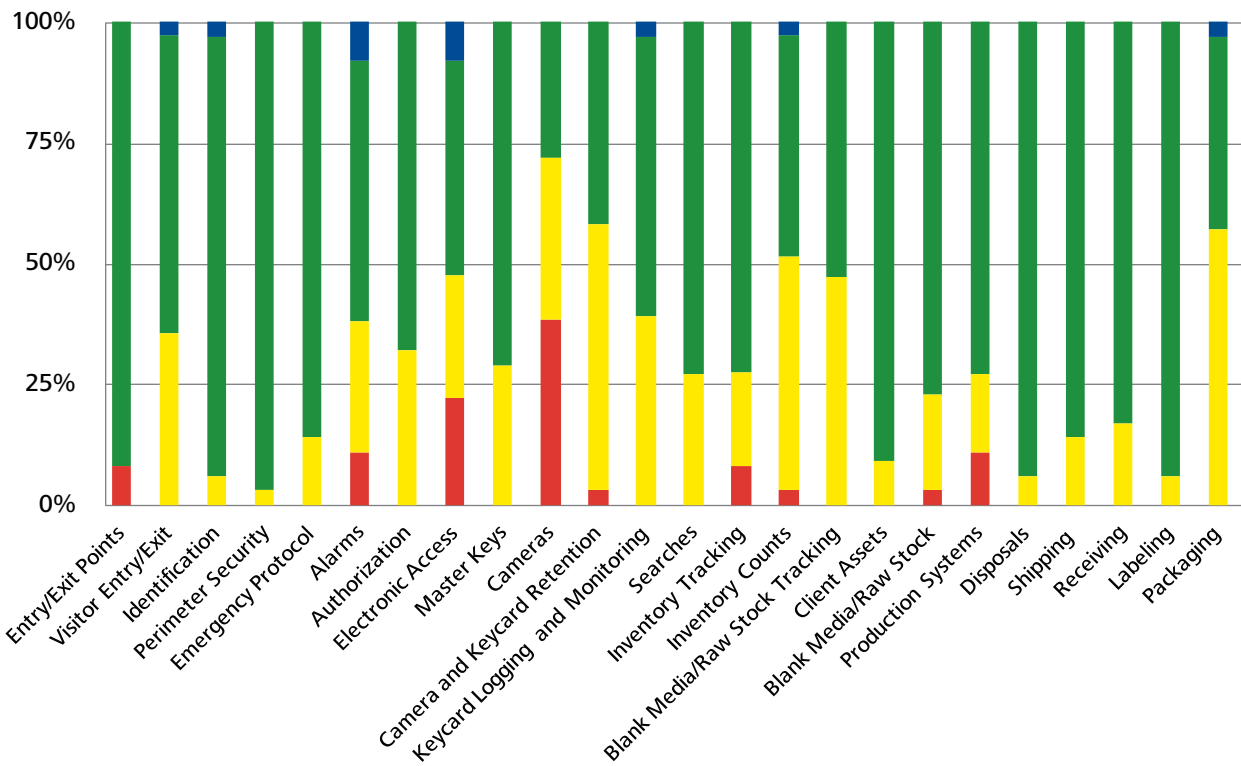


■ Exceeds Best Practice
 ■ Meets Best Practice
 ■ Improvements Needed
 ■ Significant Improvements Needed

Post-Production (cont.)

Physical Security

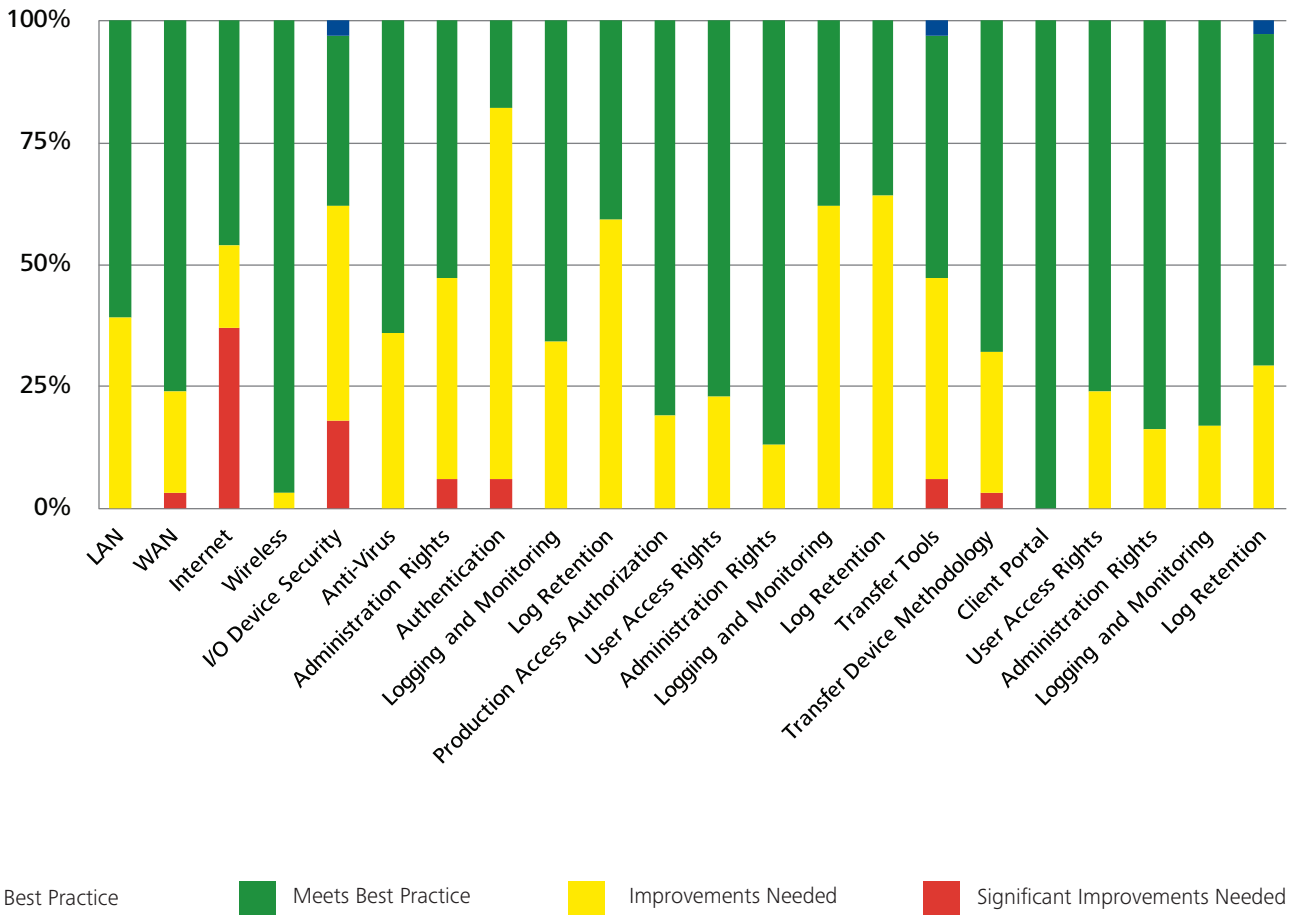
In general, vendors met best practices related to Inventory Tracking, while approximately half met or exceeded best practices related to Inventory Counts. Post-production vendors are good at tracking assets, but require improvement assessing inventory compared against system records. The vast majority of vendors met best practice for Client Assets, indicating that a vault is used to safeguard physical elements. Performance for the Camera dimension showed that improvement is needed. Consideration in yellow generally indicates that additional cameras may be needed in key areas, or adjustments made to existing cameras. However, red generally indicates that a very limited number of cameras, if any, are in place at a facility. In addition to cameras, electronic access also shows that keycard access systems may not be adequately implemented in key production areas. The combination of the two exceptions may lead to higher risk of employees entering production areas without the preventative keycard system and detective camera system.



Post-Production (cont.)

Digital Security

Digital security also showed several positives and negatives. From a positive perspective, vendors surveyed met best practices related to production access – which is dictated by unique users to gain access to content storage. On the downside, vendors overall are having difficulty meeting Internet and end-user computing restrictions (e.g., ability to secure USB/FireWire ports, DVD-burning capabilities). In general, there is considerably less maturity when it comes to digital security. This may be due to several factors. Best practices may be more difficult to attain, require significant capital investment, and tools and software used must be available and cost effective. Smaller vendors may have less IT expertise, which may lead to the underestimating of digital related risks, both internal and external. The lack of expertise may lead to less capital investment and focus on digital security.



Site Survey Trends: Audio, Dubbing and Sub-Titling

Audio, dubbing, and sub-titling sites made up approximately 11% of the sites surveyed in 2010, which is similar to previous years.

Audio, dubbing, and sub-titling sites can be further broken down into (1) those that perform audio work to support theatrical releases, including services, such as voice overs, automated dialogue replacement (ADR), and Foley; and (2) those that focus on dubbing and sub-titling related to international versioning. The facilities that focus on audio recording may receive little or no visual media, and if pictures are used for ADR, many times they are brought in for that session only. Hard drives are commonly used to transport content, and there is less reliance on central storage. Dubbing and sub-titling facilities commonly receive a highly watermarked and low-resolution picture only.


With respect to best practices, audio, dubbing, and sub-titling vendors had perhaps the lowest perceived security capabilities of the three most common vendors surveyed (Post-Production, Replication). Perhaps unlike


other post-production and distribution sites, audio sites rely more heavily on one-on-one sessions with sound editors and clients. As such, a focus is placed on physically securing sound bays that may be used for sessions, and less emphasis is placed on central storage and content tracking mechanisms. In general, elements produced on-site have limited digital tracking and are shared with clients using standard unencrypted channels (e.g., FTP).


Site Characteristics


Sites Surveyed:	11
Avg. Employees/Temps:	61
Geographic Concentration:	64% Domestic 36% International

Control Environment		Physical Security			Digital Security		
Organization Maturity	Competency	Facility	Asset Management	Transport	Infrastructure	Content Management	Content Transfer
Organization Maturity	Recruitment & Personnel	Facility Access	Inventory & Asset Management	Shipping & Receiving	Infrastructure Security	Content Authorization	Transfer Security
Policies & Procedures	Training & Education	Facility Security	Physical Asset Security	Packaging & Transport	System Security	Content Tracking	Transfer Authorization
Incident Response	Vendor Management	Facility Authorization			Infrastructure Authorization		Transfer Tracking
Process Management		Facility Monitoring			Infrastructure Monitoring		

 On average, over 75% of vendors met best practice levels

 On average, 50 - 75% of vendors met best practice levels

 On average, 25 - 50% of vendors met best practice levels

 On average, less than 25% of vendors met best practice levels

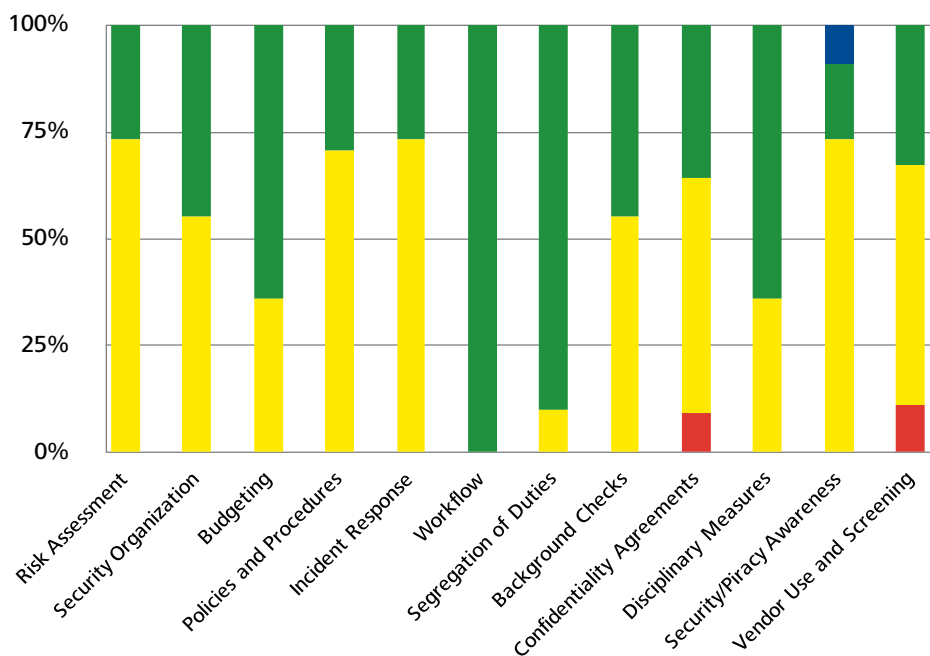
Audio, Dubbing and Sub-Titling (cont.)

Performance vs. Best Practices

The charts below are a graphical representation of the percentage of audio, dubbing, and sub-titling vendors that have met best practices for each element across the three domains of control environment, physical security, and digital security.

Control Environment

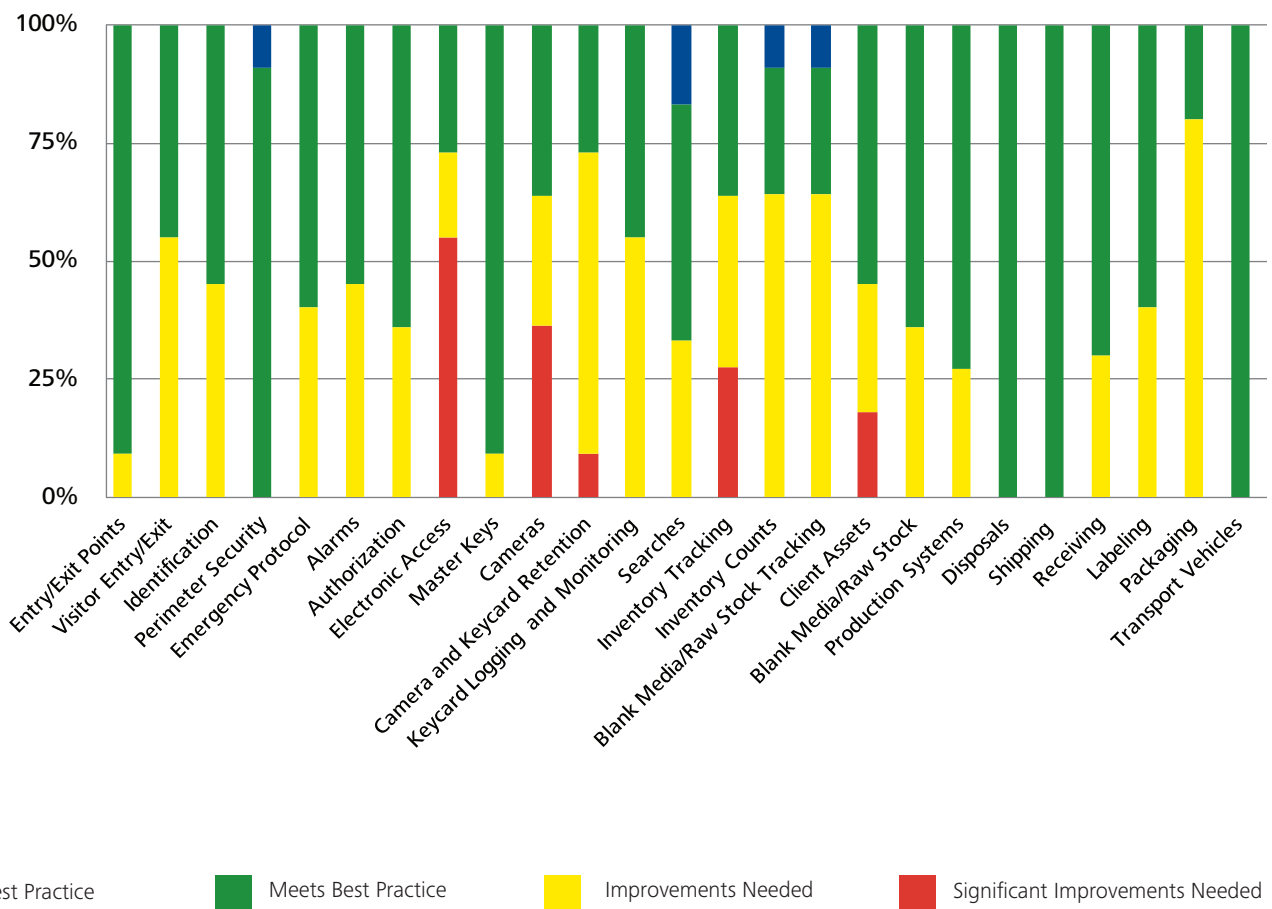
At the control environment element level, audio, dubbing and sub-titling facilities on average have greater areas of improvement when compared to post-production and replication sites. Audio facilities have among the most relaxed company cultures of the facilities surveyed and often times consist of specialists with years of experience, operating independently of the larger post-production companies.



Audio, Dubbing and Sub-Titling (cont.)

Physical Security

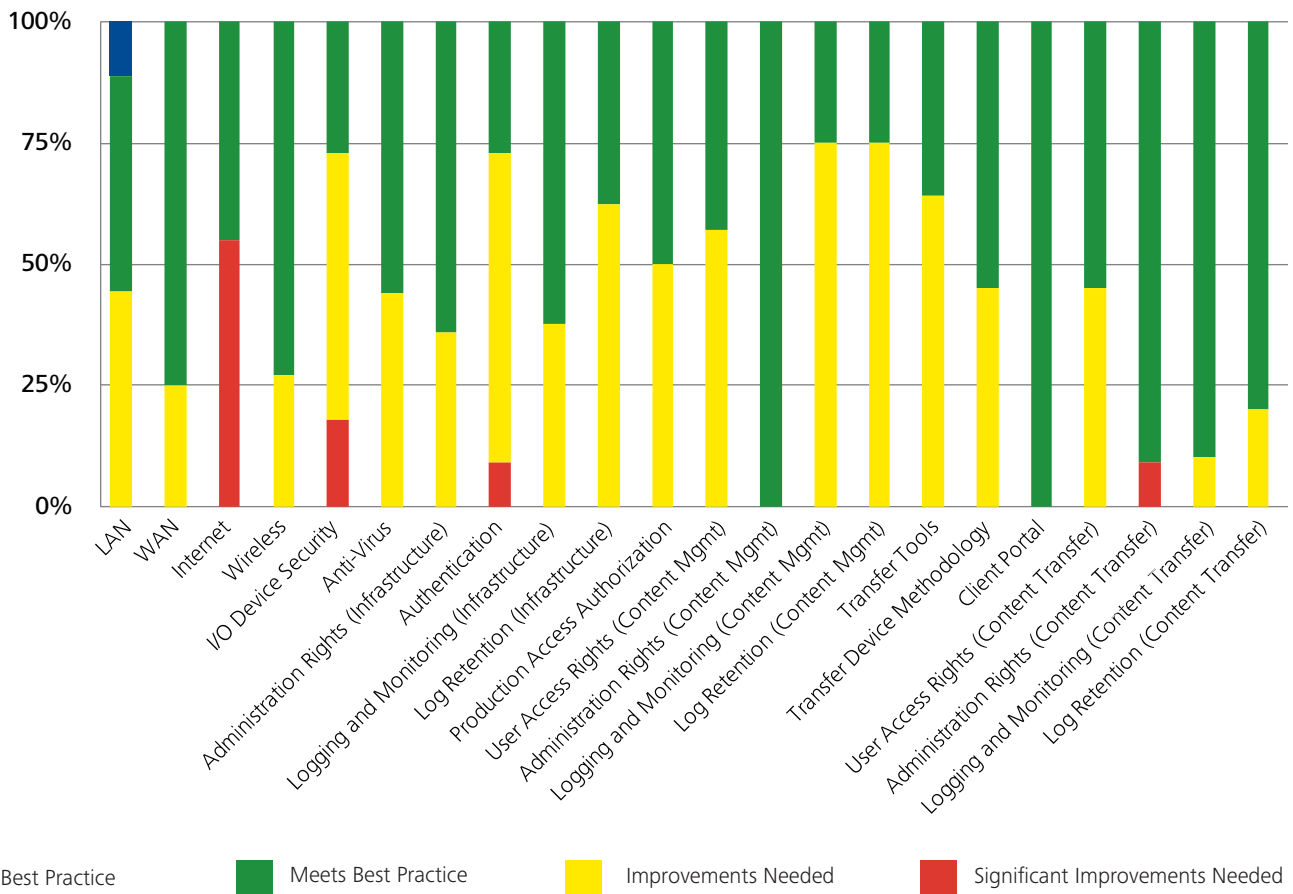
Sites scored high in areas, such as traditional facility entry/exit points and perimeter security, but improvements can be made in internal security, with 73% of sites not meeting best practices for Electronic Access - audio sites may rely more on traditional lock and key to secure critical areas rather than using access key cards. In addition, 27% of vendors had immediate improvement areas related to Inventory Tracking, which would generally indicate that client assets are not systematically tracked compared with the larger post-production companies.



Audio, Dubbing and Sub-Titling (cont.)

Digital Security

It is common to have sound suites with standalone workstations or with workstations connected to shared storage devices. Most vendors had Internet (55%) and USB/FireWire port access (73%) enabled on production workstations. As hard drives are commonly used by audio vendors to work in bays, most consider USB/FireWire to be a necessity to their workflow. Additionally, 64% are using unencrypted transfer methods (FTP) to send audio content. Audio vendors may also view this as acceptable given the perceived lower level of value associated with audio clips as compared with high-resolution video.



Site Survey Trends: Replication

Replication sites continued to make up a significant portion of sites visited in 2010, with approximately 20% of the sites surveyed. Replication sites selected in 2010 more than tripled from 2009. Of the sites surveyed, 95% were located outside of the United States.

Replication sites can be further broken down into (1) those that perform pre-mastering, mastering, and replication services (13 sites), and (2) those that focus solely on replication and packaging (six sites). The facilities that focus on replication generally only receive a stamper from a replication house that performs mastering. Mastering replication houses usually create checkdiscs. In addition, it is also common for international DVD replicators to have in-house abilities relating to DVD authoring, but these services are mainly for local productions.


The 19 sites surveyed were located across 14 countries. It is difficult to conclude on the security levels based on country or region, as many times country-specific vendors are used in later releases, after the feature has been released in the United States.


Replication risks center around loss prevention. Security in the case of replication sites must be designed almost outside in — operating under the assumption that any employee may be able to gain access to DVD content through the workflow. As such, limiting employee exit points, a strong exit search process, and securing emergency exits are paramount for replication houses.


Site Characteristics


Sites Surveyed:	19
Avg. Employees/Temps:	382
Geographic Concentration:	5% Domestic 95% International

Control Environment		Physical Security			Digital Security		
Organization Maturity	Competency	Facility	Asset Management	Transport	Infrastructure	Content Management	Content Transfer
Organization Maturity	Recruitment & Personnel	Facility Access	Inventory & Asset Management	Shipping & Receiving	Infrastructure Security	Content Authorization	Transfer Security
Policies & Procedures	Training & Education	Facility Security	Physical Asset Security	Packaging & Transport	System Security	Content Tracking	Transfer Authorization
Incident Response	Vendor Management	Facility Authorization			Infrastructure Authorization		Transfer Tracking
Process Management		Facility Monitoring			Infrastructure Monitoring		

 On average, over 75% of vendors met best practice levels

 On average, 50 - 75% of vendors met best practice levels

 On average, 25 - 50% of vendors met best practice levels

 On average, less than 25% of vendors met best practice levels

Replication (cont.)

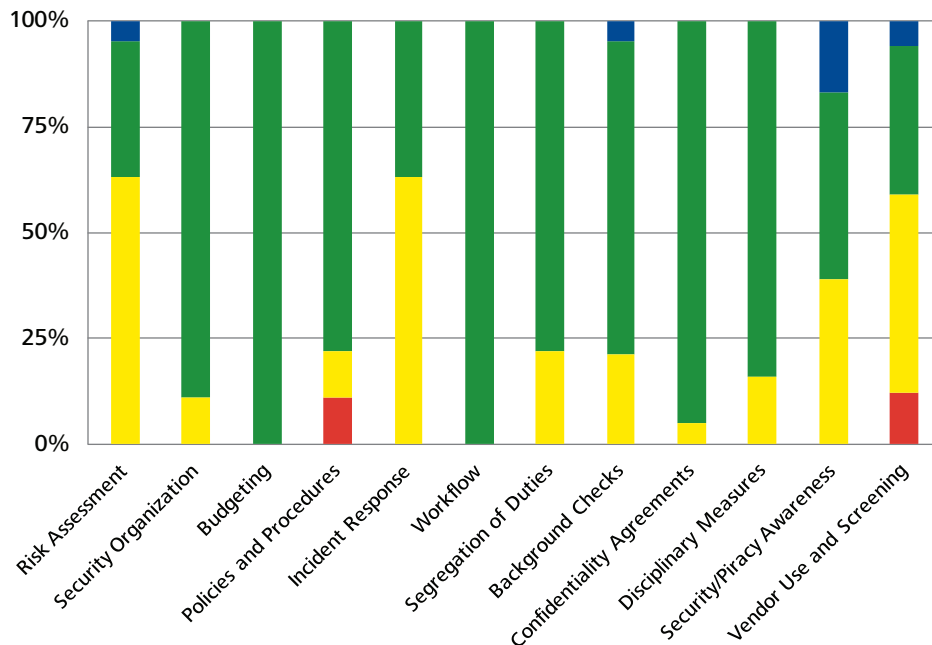
Performance vs. Best Practices

The charts below are a graphical representation of the percentage of replication vendors that have met best practices for each element across the domains of control environment, physical security, and digital security.

Control Environment

Replication facilities performed better in areas of Security, Policies and Procedures, Background Checks, and Confidentiality Agreements, with 78% or higher of vendors meeting best practices set at an element level. In order to meet best practices, areas of improvement were typically observed to be related to Risk Assessment and Vendor Management. Formal processes to assess security internally and externally (e.g., for transport vendors) require improvement.

Replication sites are more prone to have content leak attempts compared to other sites, as employees may be of a lower skill level and having less vested in the industry (e.g., compared to an editor in post-production). As such, replication sites must have a robust way to identify, handle, and escalate attempted leaks or incidents. As we see below, a majority of vendor locations surveyed need improvement in this area.

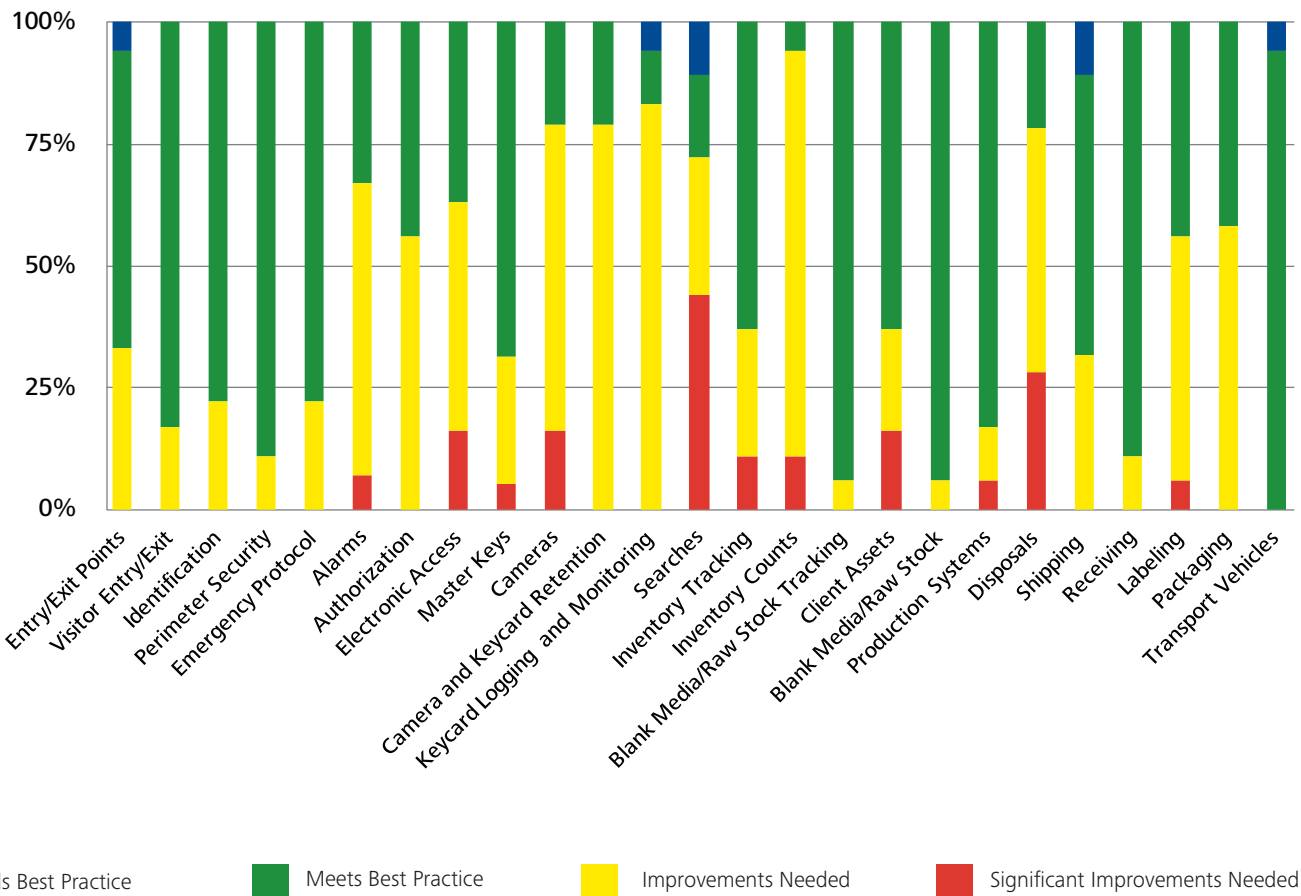


Replication (cont.)

Physical Security

On average, facility security stands out as an area for improvement for replication facilities. About 44% of the vendors surveyed received an immediate improvement consideration for their exit search procedure. This likely indicates that replication facilities have either poorly designed or no exit search procedure in place. In general, the exit search process is a good indicator of overall loss prevention controls in place, including alarms, patrols, and scrap monitoring. Eleven percent of sites, however, exceeded best practice in searches, as one replication company has implemented full body scanners to supplement the search process. The majority of vendors did not meet best practices regarding disposals – replication facilities produce scrap as a result of the replication and packaging process. This should be stored in locked storage bins and the entire process monitored.

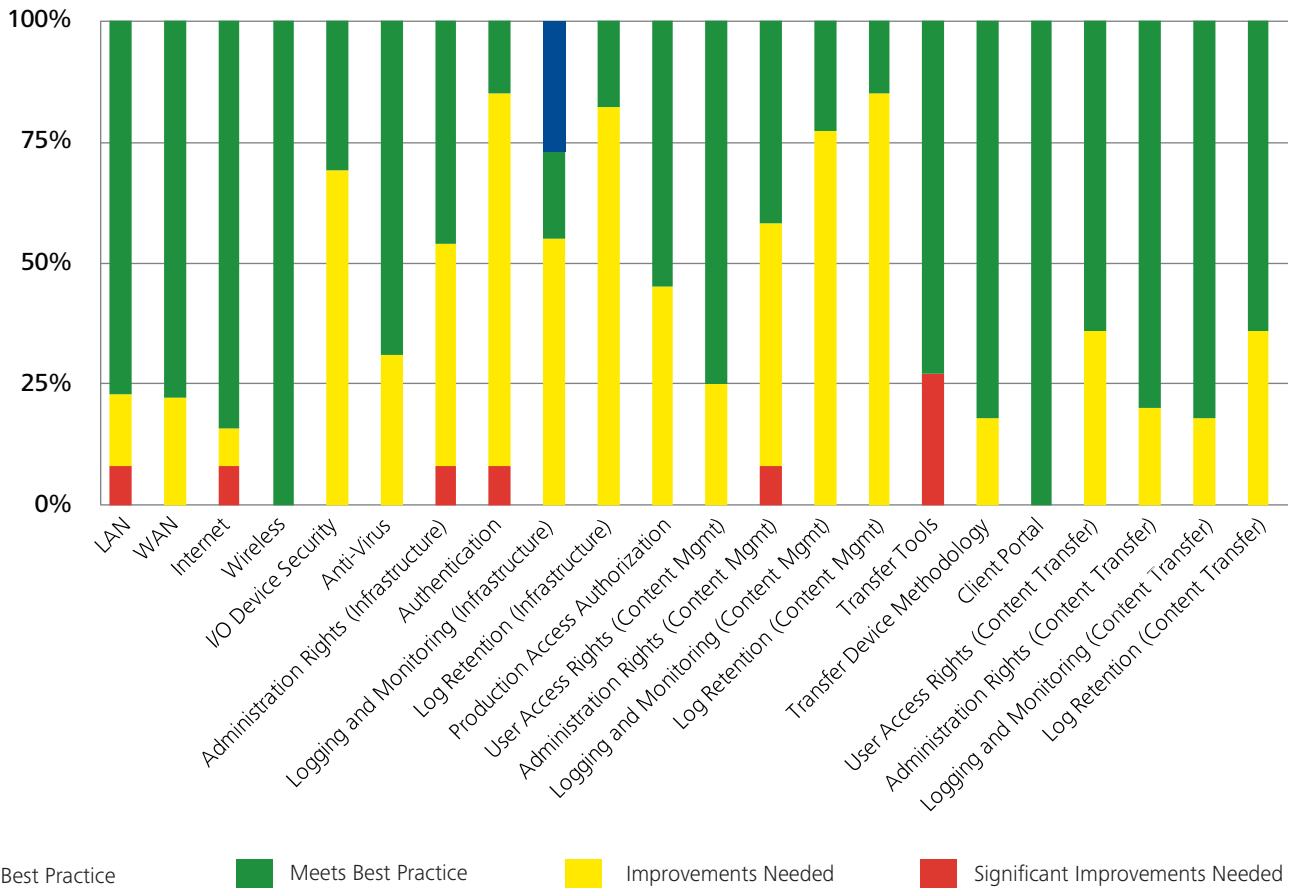
In addition to facility security and loss prevention, replication sites also need improvement in performing inventory counts for mastering material — a high percentage of sites did not meet best practices related to Inventory Counts. A lack of inventory counts may lead to misplaced stampers of high value.



Replication (cont.)

Digital Security

Digital infrastructure security typically was on par with best practices for pre-mastering facilities; mastering is usually performed in a local standalone environment. Eighty-five percent of vendors, however, had considerations related to authentication – typically personnel (across shifts) share user accounts in the pre-mastering/mastering environment. Fortunately, the vast majority of the time, the pre-mastering area in which these workstations are located is beyond access-controlled doors. From a content transfer perspective, most receive images through secure channels, but approximately a quarter of vendors continue to use unencrypted channels (e.g., FTP). A portion of replicators may be handling only post home entertainment release content and may view tighter controls over the receiving of images through secured channels as necessary.

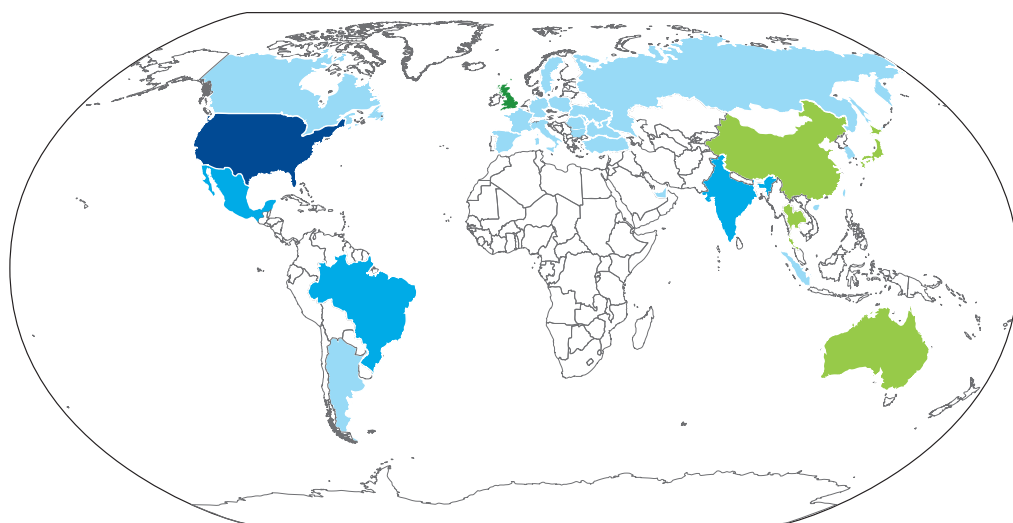
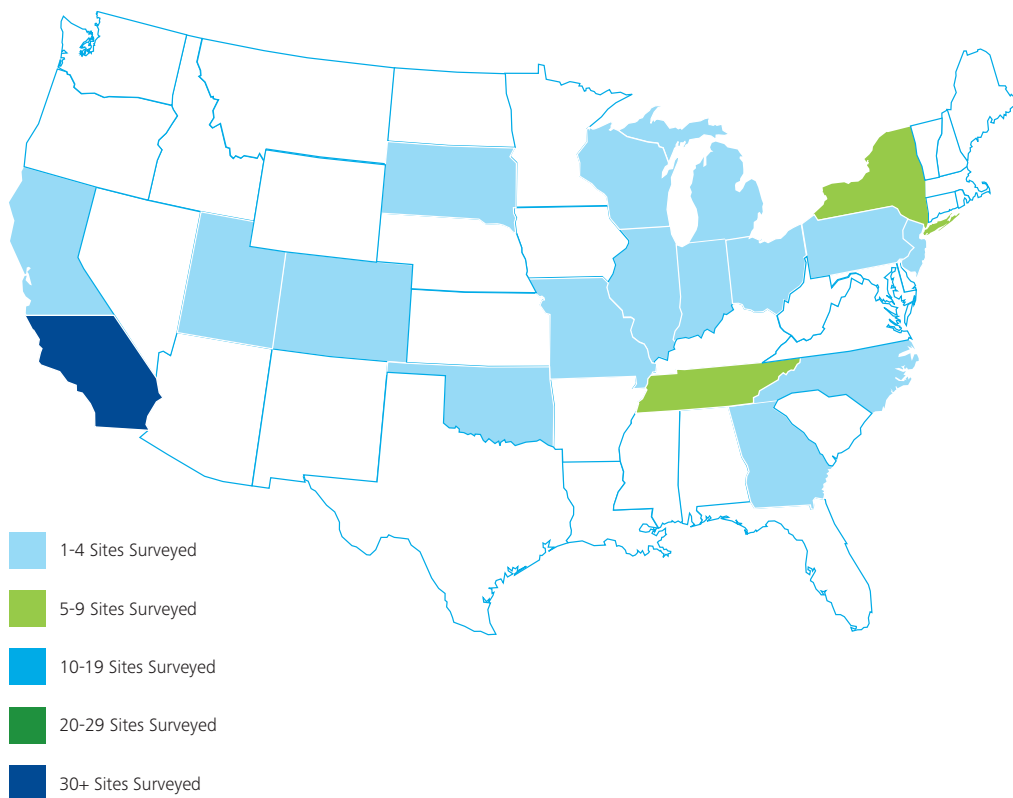


Appendix I: Geographic View of Vendor Locations

Global Reach

Since 2007, more than 303 surveys have been conducted in 32 countries – 24 countries were visited in 2010 alone.

Country	Sites Surveyed
United States	171
United Kingdom	26
India	13
Brazil	10
Mexico	10
Australia	7
Japan	7
China	6
Thailand	6
Canada	4
Russia	4
Argentina	4
Spain	3
France	3
Poland	3
Italy	3
Turkey	3
South Korea	3
Taiwan	2
Hungary	2
Czech Republic	2
Ukraine	1
Austria	1
Germany	1
Bulgaria	1
Romania	1
Belgium	1
Sweden	1
Indonesia	1
Singapore	1
Hong Kong	1
United Arab Emirates	1
Total	303



Appendix II: MPAA Content Security Model

Capability Dimension Descriptions

The MPAA Content Security Model is an assessment tool providing an analytic framework for assessing a facility's capabilities to secure content. The program assesses the facility in 25 capability dimensions across three areas: (1) control environment, (2) physical security, and (3) digital security.

Capability dimensions (e.g., Facility Monitoring) and their underlying elements (e.g., Cameras) are based on relevant ISO standards (27001/27002), security standards (e.g., NIST), as well as industry best practices.

Control Environment	Physical Security	Digital Security
<p>Organization Maturity Controls implemented by executive management that enable the organization to identify security threats, develop formal action plans, establish roles and responsibilities, and budget for the implementation of security controls.</p>	<p>Facility Access Access controls implemented at the facility in order to prevent unauthorized access, including physical entry protocols for employees and visitors, as well as means of identifying internal personnel, temps, and visitors.</p>	<p>Infrastructure Security Logical security controls implemented at the infrastructure or network layers of the production/content network. This includes network servers, routers, switches, and other network devices.</p>
<p>Policies and Procedures Formal policies, procedures, and guidelines implemented in order to minimize the possibility of inappropriate handling of assets and execution of implemented controls.</p>	<p>Facility Security Security controls implemented at the facility in order to secure the perimeter, including the use of fences/walls, alarm systems, as well as the implementation of emergency protocols to enable the company to keep client assets secure.</p>	<p>System Security The use of input/output devices has been blocked and/or is monitored on production systems where digital content is stored or processed. Antivirus software is implemented to prevent production/content network from being infected with viruses and/or malicious code.</p>

Control Environment	Physical Security	Digital Security
<p>Incident Response The process and established procedures that are followed by the organization in order to respond and minimize the impact of an incident, as well as procedures to report to appropriate stakeholders.</p>	<p>Facility Authorization Processes are implemented by the company in order to allow physical access to the facility only if approved by appropriate parties, as well as access control mechanisms have been implemented in order to restrict access within the facility.</p>	<p>Infrastructure Authentication and Authorization Authentication mechanisms have been implemented to restrict access to production/content network. Administration access rights are restricted to appropriate personnel in charge of production/content network security. This pertains to network devices, as well as the operating system on production workstations and servers.</p>
<p>Process Management A workflow is implemented by the company, including checkpoints and segregation of duties. The workflow is monitored to ensure controls remain operating as implemented.</p>	<p>Facility Monitoring A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on company's retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.</p>	<p>Infrastructure Monitoring Processes used for the logging and monitoring of activities performed on the production/content network, including routers, switches, and other network devices. Also, includes processes to maintain logs for an appropriate period of time.</p>
<p>Recruitment and Personnel The process of recruiting personnel includes controls to mitigate the risk of hiring personnel that would pose a higher threat to client assets and/or digital content. Controls can be composed of background checks, confidentiality agreements, and disciplinary measures.</p>	<p>Inventory and Asset Management Process to track inventory, use of a media asset management system, and physical inventory counts of finished, WIP, and blank media/raw stock.</p>	<p>Content Authorization Process to manage user access rights to digital content, including the processes to manage access requests, access changes, and access terminations, as well as controls to limit administration rights. This pertains to content storage devices (e.g., SAN, NAS, and content server).</p>
<p>Training and Education Security and anti-piracy training and awareness programs established by the company are given to all employees and temps upon hiring, as well as on a periodic basis.</p>	<p>Physical Asset Security Client assets, blank media/raw stock, and production systems are stored in secure locations with access restricted to appropriate personnel. In addition, scrap/disposal assets are stored in a secure location before destruction and all disposals/destructions are logged.</p>	<p>Content Security Advanced security techniques are available to be used on all client assets, including watermarking, fingerprinting, and encryption.</p>

Control Environment	Physical Security	Digital Security
<p>Vendor Management The organization follows a vendor screening process that ensures vendors emulate the organization's internal policies, procedures, and standards as they relate to the protection of client assets.</p>	<p>Shipping and Receiving Process to receive and ship assets in and out of the facility, including techniques used to track asset shipping and receiving details.</p>	<p>Content Tracking Activities performed with digital content (e.g., access, copy, movements) are tracked through the use of object audit logging and/or digital content management system. Also, audit logs are retained for an appropriate period of time. This pertains to content storage devices (e.g., SAN, NAS, content server).</p>
	<p>Package and Transport Controls are implemented to prevent assets from being targeted during the shipping process, including techniques for labeling, packaging, and transportation of assets.</p>	<p>Content Transfer Security Secure transfer tools are implemented and dedicated content transfer devices are used. If a Web portal is used for sharing content with clients, it has to be restricted to authorized users and protected by appropriate security mechanisms.</p>
		<p>Content Transfer Authorization Process to manage user access rights on content transfer tools, including the processes to request and grant access and assign system privileges, as well as controls to limit administration rights.</p>
		<p>Content Transfer Tracking Electronic transfer tools have logging capabilities enabled to monitor all transfer activities performed with digital content. Also, controls to ensure that logs are retained for an appropriate period of time are in place.</p>

Appendix III: 2010 Best Practices Overview

2010 Best practices are organized following the MPAA Content Security Model, which is used as the basis for all site security surveys. They are intended to provide current and future vendors utilized by MPAA Members with an understanding of general content security expectations and current industry best practices. Compliance with best practices is strictly voluntary.

Content security best practices are designed to take into consideration the services a facility provides, the type of content the facility generally handles, and in what release window the facility operates. There are 10 different best practices to cover different facility services. The following table shows a listing of all best practices published:

Facility Service Type	Typical Facility Services
Audio, Dubbing, and Sub-titling	Original and Foreign Language Dubbing, Sub-Titling, SFX, Scoring, ADR/Foley
Creative Advertising	Non-Finishing, Trailer, TV Spots, Teasers, Graphics
Digital Services	Digital Intermediate, Scanning, Film Recording
Distribution	Distribution, Fulfillment
DVD Creation	Compression, Authoring, Encoding, Regionalization, Special Features, Checkdisc QC
Film Lab	Negative Processing, Cutting, Release Prints
In Flight Entertainment (IFE)/ Hospitality Services	IFE Lab, IFE Integration, Hotel, Airline, and Cruise Ship Distribution
Post-Production Services (Small)	Telecine, Duplication, Editing, Audio, Finishing, QC, VFX
Post-Production Services (Large)	
Replication	Pre-Mastering, Mastering, Replication, Checkdisc Creation

Best practices are available at http://www.mpa.org/_piracyBestPractice.asp.

For More Information

Angelo Trujillo

Program Director

Motion Picture Association of America, Inc.

Tel.: +1 818 995 6600

E-mail: angelo_trujillo@mpaa.org

General Information

E-mail: sitesurvey@mpaa.org

Endnotes

i Although 95 vendor sites were surveyed, 101 reports were issued. Graphs and statistics used represent the total number of reports generated.

ii In 2010, sites were categorized into one of the 10 best practice categories. Sites in previous years (e.g., Digital Distribution, Hospitality, and Transport) were also merged.

iii Responses were placed into the general categories for illustration purposes. There has been considerable judgment in placing responses into categories, as responses many times may be vague or have mixed responses depending on the number of considerations for the element noted.

iv Please note that digital security is not applicable to certain facilities (e.g., distribution center) and the consideration count will be out of a total of 94 sites.