Managing Security in Enterprise Video
Introduction
Use of online video is increasing in the enterprise. Whether it is used for training, internal communication, or external-facing presentations, video is now a permanent fixture of the corporate information technology landscape. As such, video should be viewed as an information asset subject to security policies. Placing video into the corporate infosec program, however, has its challenges.

On one level, treating online video as an information asset is not that big a deal. It’s a digital file type that sits on a server in the infrastructure. It can be secured just like a text document. At the same time, video has several qualities that make it different from common information assets. For example, video assets tend to evolve through different life stages, such as pre-webcast, webcast, and archive. At each stage, their security requirements may be quite different. In addition, video assets are often handled by third party personnel, such as audio-video producers, and are run through dependent applications, such as webcasting tools. This paper looks at online video from an information security management perspective. It outlines some of the major threats and vulnerabilities that affect video assets. It then reviews some countermeasures that can be used to mitigate these risks.

Video is Not a Typical Information Asset
Video appears to be just like any other information asset, but from an information security perspective, it’s not. Unlike other information assets, for example, video is designed in a format that can play on CNN. Though most corporate online video is innocuous, an embarrassing or confidential video in the wrong hands can present a major security risk. From a digital perspective, video is usually opaque. It’s nearly impossible to index video content using standard enterprise search technology. As a result, video eludes many compliance and e-discovery programs. In terms of pure size and unpredictable load characteristics, too, little can match video’s potential to wreak havoc on a network if its use is not well governed.

Video is also handled by people and software that are not in the usual corporate IT processes. Video is frequently created by specialized audio-visual vendors who use their own digital equipment. In many cases, audio visual personnel are freelancers whose conduct is covered by policies and agreements that lack enforceability. Video is part of an intricate ecosystem of hardware and software. A video file may be the raw material, but its practical use occurs in live or on-demand webcasts (streams) and video portals. The interactions between all the various people and systemic components make managing security for video quite challenging.

Then, there is the issue of public consumption of the information asset. Few information assets have such a divided lifecycle as enterprise video files. Before they are published they may be highly confidential. Then, as is often the case, they are webcast worldwide. Even after such publication, however, the asset owner may not want the video misused. Unfortunately, the world has seen ample evidence of malicious and mischievous handling of media files.
Enterprise Video Risk Assessment

The exceptionalism of video from the security point of view emerges immediately when considering the standard risk assessment. What is the business impact of a risk to an enterprise video asset? Where does video belong on the business impact chart shown below? Is it in the red zone, where impact is catastrophic and certainty of an incident occurring is nearly certain? Or, does video present a minimal impact? It depends...

![Business impact chart](image)

Table 1 - Business impact of security risk chart, assigning a risk impact score based on the combination of severity and likelihood of a threat being realized. Video tends to be a low impact security risk, but has the potential to be very serious if confidential information is involved.

In contrast to conventional corporate data or documents, for which a business impact can be reasonably calculated, for video, it's variable depending on any number of circumstances. A video of the company holiday party getting posted to an intranet in violation of an acceptable use policy is a pretty minor problem. That would rank at about a 3 or 4 on the business impact scoring chart. A video of a senior executive disclosing embarrassing or confidential information could be a security incident with high business impact. If the risk has not been mitigated adequately, the impact could climb into the red zone, with high likelihood and high severity.

The difference between low and high security risk for video is due mostly to the unusual nature of video assets. Enterprise video typically exists in one of two states that are relevant to security:

- **Pre-publication** - Before video is webcast or published on a video portal, its content usually needs to be kept private. Related files and information, such as PowerPoint decks, also need to be guarded.
- **Post-publication** - Once material has been made public, it is no longer confidential. That said most entities still want to control the use of video assets even if they have been webcast worldwide. And, some video assets are only semi-public. They are for internal consumption.

An example of this pre/post publication dichotomy is the security challenge facing a company that wants to webcast an important, sensitive news announcement, such as a merger. This kind of news can affect the stock price of a company and it is subject to compliance with SEC laws. In the pre-publication phase, where webcast producers are preparing presentation documents and scheduling presenters, the content of the webcast must be kept confidential.
After the webcast, confidentiality no longer matters. The business impact of security risks on those video assets will drop precipitously.

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Impact Rating</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Media Files</strong></td>
<td>- Unintended disclosure</td>
<td>- Media server</td>
<td>Variable</td>
<td>Access controls on media server, storage, content management and webcasting tools</td>
</tr>
<tr>
<td><strong>Confidential information</strong></td>
<td>- Unauthorized use, post webcast</td>
<td>- Media storage (on-premise and cloud)</td>
<td></td>
<td>Server activity logging</td>
</tr>
<tr>
<td><strong>Personal information about presenters and producers</strong></td>
<td>- Unauthorized access, pre-webcast</td>
<td>- Webcasting tool</td>
<td></td>
<td>Contractual terms</td>
</tr>
<tr>
<td><strong>Video related Metadata</strong></td>
<td>- Unwanted modification.</td>
<td>- Video content management tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Stream</strong></td>
<td>- Eavesdropping</td>
<td>- File upload stage</td>
<td>Variable</td>
<td>Access controls on media server, storage, content management and webcasting tools</td>
</tr>
<tr>
<td></td>
<td>- Misuse</td>
<td>- Third party personnel access</td>
<td></td>
<td>Server activity logging</td>
</tr>
<tr>
<td></td>
<td>- Denial of service</td>
<td>- Third party equipment</td>
<td></td>
<td>Contractual terms</td>
</tr>
<tr>
<td></td>
<td>- Unintended disclosure</td>
<td></td>
<td></td>
<td>Digital Rights Management Technologies</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Flooding</td>
<td>Peer-to-Peer stream sharing</td>
<td>Serious</td>
<td>Dedicated, restricted media players</td>
</tr>
<tr>
<td></td>
<td>Denial of service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 2 - Asset/Threat/Vulnerability/Countermeasure chart for enterprise video*

Table 2 summarizes the major information security risks for enterprise online video assets. Following standard security management process, the chart matches specific threats to the information assets associated with enterprise video. Then, it describes possible vulnerabilities and countermeasures to mitigate those threats. For example, personal information about presenters on a webcast needs to be protected from the threat of unauthorized access. The vulnerabilities that create this exposure might include deficient access controls on the webcasting tool. The countermeasures include implementing strong access controls on the webcasting tool, server logging and contractual terms. In the latter case, given the number of third parties who can be involved in webcasts, it may be necessary to make guarding of confidential information part of the audio visual service provider’s contractor agreement.

Security risks for enterprise video information assets touch on the three main areas of concern for security managers, though with varying levels of severity:
Managing Security in Enterprise Video

- **Integrity** – Organizations do face a risk that video assets will be subject to improper modification or degradation, with the result that the asset can no longer be trusted as having high integrity. However, this risk is generally perceived to be low in likelihood.

- **Availability** – If the network and application architecture for the video solution has been well designed and implemented, and is subject to governance, there should not be too much for availability. There is still risk of flooding and network overload, however, if there is a breakdown in security policy, such as an error in dev/test/production environments that leads to uncontrolled peer-to-peer sharing of video. Also, availability of enterprise video is either a non-issue or a white hot, make or break disaster. Most of the time, if a video is not available, few people are concerned about it. The recovery time objective for a video system could be measured in hours or even days given its relatively low business criticality. However, in a live webcast featuring a senior executive, an outage of even thirty seconds can be catastrophic. In general, the best practice is to assure high availability for live webcast events.

- **Confidentiality** – Most security risks for enterprise video assets involve confidentiality issues. Like the availability risk category, confidentiality for video assets is usually either minor or very serious, depending on context. Given the potential for serious impact from confidentiality threats, it is advisable to implement strong countermeasures for confidentiality.

Compliance and e-discovery are two other categories that need attention when assessing risk for enterprise video assets. Video assets need to be included in any program for data lifecycle management. Just like other information assets that could be considered electronic evidence in legal matters, video files need to be capable of data custodianship and chain of evidence processes for e-discovery.

**Risk Management for Enterprise Video**

Risk management for enterprise video is a subset of the broader information security programs of the organization. When discussing specific video-related security measures, it should be an absolute requirement that the video assets are subject to all of the organization’s general security policies, standards and controls. For example, media servers have to be subject to hardening standards, password encryption rules, patch management processes as any other server in the data center. Similarly, video assets should be governed by organization-wide policies on acceptable use, privacy and confidentiality. Mitigating risks to enterprise video is a practice that falls into three categories that reflect the participants and activities that occur when video is webcast to an audience. There is risk mitigation for the audience side of the experience, the authoring process, and the streaming process.
Risk Mitigation: Audience Side

The two basic risks to enterprise video assets on the audience side involve confidentiality of audience members’ personal information and use of the video material itself. If a webcast is completely public, neither of these are issues. However, in most cases, an organization will want to control who is seeing their video assets. To do this, they rely on webcasting and video portals that require personal user registration and login. The personal information about these users needs to be protected from improper access, use, and disclosure. Two countermeasures make this possible:

- **Integration of the video tool with identity management and access control systems** – Assuming the organization’s identity management and access control systems (such as LDAP) are secure, then assigning video access privileges through such a system will minimize the chance of private user information being accessed on the video tool.

- **Controls over video tool** – If personal information about registered viewers of video assets resides on the video tool, then that tool must have adequate controls to mitigate the risk of improper access to personal information. If the video tool has been provisioned in accordance with enterprise security standards and policies, this should provide satisfactory mitigation of the risk that personal information about video viewers can be compromised. However, there are several security issues that can arise from architectural considerations, including:
  - **The database and application structure of the video tool** – Though the video tool may appear to the end user as a one seamless application, it is invariably comprised of a fairly intricate set of backend applications and database elements. Though none of these elements present a major security concern if they are deployed in accordance with enterprise security standards, it is necessary to understand exactly what makes up the video tool and how data in it might be compromised. For example, most video tools interact with separate, usually third party media servers (such as Adobe Flash Media Server or Microsoft Windows Media Server.) The security manager has to be aware of these connections and how data is safeguarded while in transit between elements.
  - **Cloud-based components of the video tool** – Locating some or all of the components of the video tool in the cloud has become a common practice today. Again, this may not present a serious risk exposure if the deployment is understood by security managers.

In some cases, video is published without concern for who will see it. Much of the time, however, a webcaster wants to have control over who can see a video. This is true for live video presentations as well as those that are stored for on-demand viewing. Countermeasures to mitigate risk of unauthorized or improper access to video assets include the following:

- **Access controls for video content** – Video assets can and should be password protected. Beyond that, it is optimal if the video tool has the potential to authenticate
and authorize viewers, perhaps through integration with access control systems such as LDAP.

- **URL Restrictions** – The video tool should be able to restrict viewing of the video to a select set of URLs. With this control, it will be impossible for the video to be viewed through unauthorized sites.
- **Security Assertions** – In cases where video can viewed on a private portal but also shared publicly, it may be necessary to embed a security assertion (e.g. SAML) to ensure that a private video is not improperly made public. The security assertion will allow authorized people outside the firewall to view the video but restrict those who are not.
- **Player Restrictions** – Some video tools enable video publishers to restrict the viewing to just one type of customized media player. This creates a control where only those who have been given access to the specified player can view the video.
- **IP Address Restrictions** – the video tool should be able to restrict viewers to designated IP address ranges.
- **No Caching of Media** – In the best case, the player and video tool should prohibit caching of video on the local machine. This will reduce the risk of video being viewed without permission.
- **Digital Rights Management (DRM) Tools** – Can be deployed to manage video access after publication.

**Risk Mitigation: Authoring Side**

A number of security risks emerge in the process of preparing and webcasting video and related assets, such as PowerPoint decks. In general, if the video tool and media servers have been deployed in accordance with enterprise security standards, much of the risk of unauthorized access to the video authoring process will be mitigated. However, it is important to note a few specific risks that need to be dealt with on the authoring side:

- **Access Controls for Video and Related Assets, Pre-Presentation** – The video tool usually has functions for preparing a live or on-demand webcast presentation as well as for managing the event itself. This system must have strong access controls and logs. It is possible that highly confidential material will be uploaded to the video tool before the video is published. Access to the database elements of the video tool needs to be tightly controlled.
- **Transfer of Assets Up to the Video Tool** – The upload of materials to the video tool needs to be secure with mitigation of “man in the middle” type attacks and other forms of eavesdropping on network traffic.
- **Reliance on Third Parties** – Video production often involves numerous third parties, such as camera operators, editors, video producers, and others. These people, or companies, need to be subject to whatever security policy has been created for outside entities. Policies might include such things as a requirement that they sign certain types of non-disclosure contracts and carry errors and omissions insurance.
Risk Mitigation: The Stream
Streaming media is one aspect of video that makes securing video assets different from conventional security practices. In streaming video, a media server sends a stream – essentially chunks of the media – out to players, where they cache and are viewed. The movement of data in the stream presents several security challenges which must be addressed if there is a concern about the confidentiality of the video.

- **The Uplinks and Downlinks** - It is necessary to understand the network connections that are being used to flow video streams from the encoder to the media server and from the media server out to the player. Each hop needs to be secure.
- **Encryption** – It may be desirable to encrypt the stream. Some video tools have this feature.
- **HTTPS/SSL** – At the transport level, the video tool should have the capability to stream video through HTTPS/SSL.
- **Peering** – Some new streaming technologies, such as multicast fusion on the Adobe Flash Platform, enable peer-to-peer sharing of video inside an enterprise. This may sound like a bad idea given the history of P2P on the Web. However, with the right tools, such as Adobe Rendezvous Server, it is possible to have secure and manageable peer assisted content delivery.

Conclusion
Managing security for enterprise video assets is not the most difficult challenge that a security manager will ever face, yet the process is not entirely routine either. The good news is that a well implemented enterprise security policy will help mitigate many of the risks inherent in managing video assets. At the same time, video throws a number of curve balls at the security manager. These include dealing with numerous third parties, somewhat unusual system architectures, and a media stream that often flows outside the firewall. Add to that the highly variable levels of risk – from minimal to catastrophic – and it’s easy to see how managing security for enterprise video takes work. Selecting the right video tools and partners can make a big difference in how effective and labor intense the security process will be for enterprise video.

About MediaPlatform
MediaPlatform, Inc. is the leading enterprise webcasting solution and video portal for corporate communications, training and collaboration. MediaPlatform provides a robust video content management portal that can be deployed from the cloud or on-premises to help organizations make their business more social and improve employee engagement. MediaPlatform customers include Adobe, Ericsson, Ernst & Young Facebook and General Motors.