Protecting Digital Assets in the Modern Organization

WinEncrypt

WinEncrypt™

Protecting Digital Assets in the Modern Organization

What are digital assets?

Any text document, video or audio file, image in an electronic form, with the right of using it, is referred to as a digital asset. A digital asset can be owned by a company or an individual. A company can create its own digital assets and can even buy them, along with the sole rights to using them. Digital assets also include animations and scanned documents initially created by the employees of the company. As companies own the copyright to their digital assets, anybody caught using them in any form is liable for legal action or penalty as per company norms.

Growth in Digital Assets

With almost every organization having its a web presence, the number of digital assets is growing by leaps and bounds. The ownership of increased digital assets adds to the value of the organization, not only in terms of its reputation but a corresponding increase in customers and suppliers. Organizations are becoming progressively more conscious of the growth of Intellectual Property Rights, along with sole ownership to use such property, which leads to an increase in digital assets.

Why should digital assets be protected?

With cyber crime on the rise, it is the need of the hour to protect digital assets from being used either in same or a different electronic and/or non-electronic format by unauthorized persons. Cyber criminals are always on the look out for digital assets, especially of renowned organizations, which they can use illegally for personal gain, such as selling modified copies of the content of media in the form of some other electronic media. There is a wide assortment of electronic tools available in the market today, some of which can even be downloaded free of cost from the internet and used to change the format of digital assets belonging to others.

Access to the digital assets of a company by cyber criminals does only ruin the organization's reputation but also impacts its business. This also leads to strained relationships with business partners, customers, suppliers, contractors etc. According to a report released by the International Crime Complaint Centre in 2007, more than 1 million cases of cyber crime had been reported in the United States alone, with an approximate monetary cost of $647 million.

Ways to protect digital assets in modern organizations

Organizations are now facing the big challenge of protecting their digital assets from prying eyes. Not only are organizations devising their own methodologies and strategies to protect and manage their digital assets, but companies are spending huge amounts of money to buy asset management tools. Increasing proliferation of digital assets has made it necessary for

companies to devise best practices to safeguard their digital assets. Some of these best practices include:

Encryption software: With more and more proprietary and sensitive information being stored on digital media and with the growing population of the mobile workforce, the danger of devices being stolen or lost has increased tremendously. While the physical device can be recovered, the sensitive data once stolen can lead to unimaginable harm. The use of reliable encryption software is the best way to ensure that the data is translated into an unreadable format and becomes inaccessible to unauthorized persons..

Full disk encryption (FDE) is the safest way for business executives and professionals to protect their digital assets. Through FDE, the entire hard drive is encrypted and the user has to bear only the loss of hardware, without worrying about the data being used for illegal purposes. FDE is beneficial in terms of:

- ✓ Increase in productivity
- ✓ Centralized and organized management
- ✓ Elimination of user error
- ✓ Improvement in trust relationships with customers and business partners
- ✓ Protection against loss of data
- ✓ Protection from non-compliance penalty
- ✓ Promotes brand image

Full disk encryption provides complete protection to the digital assets by encrypting them in an algorithmic code that others would be unable to understand. There isn't any requirement for user interaction in FDE. Moreover, depending upon the requirement and infrastructure setup of an organization, the recently developed system of encryption based on hardware can also be adopted. This not only saves CPU time, which leads to an increase in system speed, but also ensures proper security.

DAM or Digital Asset Management: is a widely implemented content management strategy and a powerful software and/or hardware tool with a host of generic functions. DAM enables employees and business executives organize, manipulate, download, search, archive, optimize, verify, deliver, secure and manage the digital assets of the company. A user can also integrate his/her digital assets with third party tools using Digital Asset Management Systems**.**

The successful deployment of DAM has enabled professionals to understand the importance of protecting as well as managing their digital assets. With the increase in the demand for DAM across the globe, the number of solution providers, who develop reliable DAM software that is compatible with various operating systems, has also grown. As per the requirement, solution providers develop software that enables business executives to protect their digital assets in the best possible manner.

Companies with a large database and network structure might opt for in-house solutions for protecting their digital assets. Developing in-house DAM solutions requires more infrastructure,

staff and capital investment. Some organizations also choose to hire DAM experts in their attempt to safeguard their digital assets.
Benefits of DAM:

- ✓ Increase in productivity
- ✓ Ease in administrative tasks
- ✓ Reduction in the cost of storage
- ✓ Enhanced access and increased control over the use of assets
- ✓ Reduction in turnaround time
- ✓ Ease in decision making with organized interface
- ✓ Reduced email traffic
- ✓ Increased output through improved communication

Furthermore, in order to organize multimedia files, specific 'Media Asset Management' tools are also gaining popularity.

Enterprise Content Management (ECM) has recently been introduced as an improved strategy for managing and protecting digital assets. But there are some drawbacks associated with this method. ECM is quite expensive, making it a second option for most companies. Moreover, ECM is too complicated and IT professionals prefer not to deploy it as the preferred asset management system.

The Artesia DAM system is a good way for users to ingest, index, archive, secure, search, edit, relate, convert and distribute data in an effective manner.

Disable right click: One of the widely used but not very effective methods of protecting digital assets from being stolen and used in another format is to disable right click. If right click is disabled, it does not let the criminal copy the assets and use them for monetary or other purposes.

Implementation of Laptop Security Policy: Digital assets can be effectively protected by the successful implementation of a laptop security policy that holds all employees accountable for the digital assets assigned to them. Employees should be made to sign a written document, i.e. security policy, containing the best practices to be followed in order to protect the laptop or its data from being stolen. Effective deployment, accountability as well as scheduled audit trials should be in place to ensure the proper implementation of the policy by all members of the organization.

The security policy should also include USB flash drives or any other portable data storage device being issued to the employees that contain company data.

Conclusion

Nothing can make up for the damage caused by loss of sensitive or proprietary information. Hard drives are recoverable but trust and reputation are more difficult to re-instill in the consumer. The investment in adequate security seems a small price to pay to avoid exposing one's organization to the risk of legal action and lost reputation.