



TenStep Supplemental Paper

7 November 2008

Safe 'N' Sound

Human Capital Management (HCM) in collaboration with e-learning can successfully usher change initiatives to guarantee increased productivity and reduced costs. Feature-rich functionality and access to mobile learning environments -organizations cannot ask for anything better.

Today, there is no looking back for this 'HCM- e-learning' collaboration thanks to exponential technological advancements. Nevertheless, even as this area continues to develop, one critical issue has remained largely unaddressed. This is the importance and strategies to protect knowledge assets.

As Human Capital Management shoots to fame, protecting sensitive data used to develop content necessary for HCM initiatives becomes a rising major concern. This however, does not seem to be on the agenda of many organizations. Since novelty and innovations alone help secure the much-desired competitive edge, the issue of protecting educational content needs to be addressed immediately.

For all the differences

Government establishments and private businesses have different security objectives. Most of the information including training content in Defense and National Security agencies is highly classified. These agencies cannot even afford to let out information on their standard operating procedures and case studies.

While governments realize the benefits of e-learning powered HCM initiatives, the problem is that most agencies use a common model for their Learning Management System and content distribution. This increases the risk of leakage of classified information including sensitive learning content.

Can these agencies prevent such leaks even while availing the benefits of HCM? Yes they can, provided they implement standards like training certifications to control the distribution of classified information. While such certifications shield the transmission of sensitive data, it is equally important to protect the flow of sensitive information from creation right down to the end user. Verification of end users is a step towards this direction.

Private concerns

Most businesses in the private sector are heavy users of HCM and e-learning technologies. However, when it comes to securing their knowledge assets most fail to see the need to deploy any security measures. The only businesses that comply are in the pharmaceutical and health care industries. They consider it more of a legal requirement.

However, with the rise in competition and globalization, there is bound to be a simultaneous increase in litigation even in regulation-driven businesses. This alone is reason enough to think hard about security. Additionally, private companies must also



TenStep Supplemental Paper

consider the competitive risks they undertake when information on corporate goals and objectives, product launches and descriptions are freely accessible in cyberspace.

These businesses must therefore subscribe to new principles and regulations that underline the importance of HCM security. Although most countries have ignored such regulations, industries must together determine certain standards to safeguard their knowledge assets.

In the right direction

Many businesses have woken to the idea of securing their knowledge assets, but their approach is not right. They tend to focus on the protection of data transmission and network security alone least realizing that sensitive data needs protection right from the word go to the end user in the consumption stage. The private sector too needs to brace up like government agencies and address security concerns with sincere and determined efforts.

Experts recommend user certification as it protects learning content from improper access. Business owners might argue that scrutinizing users with stringent screening procedures may not make much business sense as they might eventually lose some of their clientele. However, it makes better business sense to weigh the risks of granting free user access than screening users.

User certification involves a series of extensive screening procedures. A user is granted access only after his identify is verified. This verification is mandatory whenever the user accesses a learning module.

Step-by-step

According to recent statistics, nearly 80 percent of security violations are inside jobs. What compounds the problem is either an absence or lack of security measures making HCM initiatives highly vulnerable to leaks. This then creates an opportunity for even those who should not have any access to critical information to access it with a click of the mouse.

The issue of securing knowledge assets can no longer be taken with a pinch of salt. Organizations must follow a systematic approach to ensure that their educational content remains intact. The security conscious recommend the following steps to address the issue.

Step one: Risk analysis. It is imperative that organizations evaluate the value their HCM initiatives provide against the inherent risk of making learning content freely available. The evaluation helps them assess criticality of their learning content.

A complete evaluation would include assessing the people involved, technology used and processes adopted. Also, if the content is extremely sensitive it is important to determine whether access to required information will really enhance the job performance of the individual. Experts recommend screening individuals to determine their need and usage.



TenStep Supplemental Paper

Step two: Follow up. Learning content must reach the desired destination or end user undamaged. While IT departments are well versed with access procedures and network security, the field of user access needs further development. Most organizations rely on certifications to verify user qualifications. These certificates however only verify the device (PC, laptop) in use and hardly help in determining the identity of the actual user.

More and more government agencies are opting for biometrics solutions where the users identify is verified usually through fingerprints to ensure selected access to sensitive information. The private sector too can follow suit.

Step Three: Unification. Tying the learning content creation process to the function of information security ensures that security procedures are adhered to at all stages (from creation to end user). In the past these functions were performed with different levels of accountability. It is important to ensure that both content creation and security procedures share common objectives and perform in tandem.

This systematic approach will protect sensitive learning content from passing into insensitive hands!