ControlPanel GRC

SYMMETRY™

CONTROLPANEL GRC ALWAYS AUDIT READY™ SERIES:

HR Data Security

Protecting Sensitive Human Resource Data: A More Secure Approach

With so much emphasis on procuring and retaining talent in today's highly competitive business environment, basic functions like ensuring the security of sensitive human resource (HR) data is not something you should have to worry about. Yet, the increasing pace of new regulations, such as the HIPAA requirements, are placing more strain on HR departments to monitor usage and prevent unauthorized access to an ever wider range of HR information. At the same time, access to information is ubiquitous in the mobile, social, "always on" culture in which all businesses must operate today. Especially for the younger portion of your workforce, access to all kinds of information, personal and otherwise, is taken for granted. In this environment, securing sensitive HR information is as much about protecting against inadvertent curiosity as it is about preventing malicious intrusions. New strategies are required to address the current cultural factors and the many new online access options. Additionally, a new approach is needed to augment and extend SAP® HCM capabilities to secure HR information, monitor its use, and prevent inappropriate access.

About ControlPanel^{GRC} HR Analyzer

ControlPanel^{GRC} HR Analyzer is a new module for SAP HCM users looking to monitor and protect employee data. The software provides three core areas of functionality: 1) HCM usage analysis – the ability to track infotypes or screen views from anyone accessing sensitive HR data; 2) enhanced employee provisioning – synchronizing employee events like new hires, title changes and terminations with SAP Users and passwords, resulting in a one-step update; 3) data scrambling – the ability to scramble any sensitive HR data in SAP quality and development systems. Part of the ControlPanel^{GRC} compliance automation solution, HR Analyzer can be used in conjunction with other modules or on its own.

What is "Sensitive" Data?

HR data is some of the most sensitive, confidential and proprietary information stored in your enterprise resource planning (ERP) system. Companies go to great lengths to isolate this data and prevent unauthorized access. Yet one of the underappreciated challenges in managing HR data security is determining what is or is not sensitive data. Not only is this a business decision, which is subject to revision with changes in key management, mergers and acquisitions, or unfavorable experiences, it also is subject to changing state and federal regulations.

While it may be obvious that data such as compensation and benefits information is sensitive, or that information like an employee's manager or work e-mail address may not be, there are many gray areas. Relying on lower-level or newer HR personnel to make those determinations and keep up with changes, or worse yet, for IT personnel to do this, is a recipe for failure. And failure to adequately protect sensitive information can have serious consequences.

On the other hand, there is great need to access HR data across the organization. HR personnel, line managers, payroll and accounting personnel, claims administrators, IT help desk staff, security guards and many others may need access to varying levels and types of HR data. For example, an HR administrator may need access to employee records within their division or business unit, but should not be accessing HR data from other business units. And they should not be accessing their own information. One company reported an incident where an HR administrator accessed their own performance review file and a co-worker's review prior to her own review, resulting in a nasty review session.

Another concern is IT staff and database administrators with privileged 'system' user rights who can view HR data as part of their job managing complex ERP systems. They often have unlimited access to all information stored in the ERP database. While SAP HCM audit trails may prevent them from changing this sensitive data without others knowing about it, it does not prevent them from viewing the information and copying it down for their own use. Even if there is no malicious intent, this is how leaks and rumors get started that can quickly poison the atmosphere within an enterprise, harming morale and productivity, as well as causing compliance problems with regulations such as the aforementioned HIPAA.

Clearly, long gone are the days when you could lock up your HR files in a cabinet and go home for the night. Now HR information must be accessible online to many different constituents, yet secured and monitored 24/7. This requires advanced security automation tools such as ControlPanel^{GRC}'s HR Analyzer™. And while HR security breaches may not fall under the category of audit risks – ControlPanel^{GRC}'s traditional focus - they can, nevertheless, hurt efficiency and cause compliance issues that can risk the health of your business.

Add / Change / Deletes are no Longer Just Add / Change / Deletes

It used to be when HR performed a routine personnel function such as hiring new employees, processing new job assignments or promotions, recording salary or rate increases, or terminating employment, they simply recorded the change in the HR system and that was the end of it – a simple add / change / delete transaction. Not anymore. Since nearly all employees now need online access to their own HR and benefits data, as well as that of any employees who may work for them, the new or updated information must be passed to others in the organization such as IT so the necessary user IDs, passwords, and security clearances can be set up for the employee. If this is a manual process, it raises a security risk and can delay the on-boarding or change process, extending the time to value for the new, transferred or promoted employee. Worse yet, if the action was a termination for cause and access is not immediately blocked, there is significant risk of reprisals and other mischief.

What is needed is a new automated approach that automatically integrates the add / change / delete process with all related actions that must be taken as a consequence of each change. This ensures all HR actions are immediately reflected in related systems so time to value is greatly improved while HR data remains secured. This is another function and benefit of HR Analyzer.

When Security Goes Out the Window

Many HR executives would be surprised to learn that normal IT test procedures can compromise their well thought out and executed HR security. It is common practice for

IT departments to run multiple versions of SAP applications and data. There are always separate development and test versions of the systems, and often one or more back-up versions available for restoring production if there are system failures and for disaster recovery. To run these systems and verify they are working properly requires data. Usually this involves copying all or subsets of production data into test and development systems as the most expedient way to compare results between versions. The problem is these extra copies of real production data, including sensitive HR information, are often not subject to the same security controls as production systems. Thus, your carefully crafted security "goes out the window."

To mitigate these security risks, companies sometimes write data scrambling routines so sensitive information is not accessible by casual users. There are three main challenges with this approach. First, since data has to be exported from the SAP HCM files before it is fed to the scrambling program, it is temporarily available in its native form. Second, since the routines are written in-house, they can easily be reverse engineered, thus undoing the presumed security. Third, in-house routines are typically best known and understood by their authors. When the person or persons who first wrote the scrambling routines move on to other assignments or leave the company, that knowledgebase is lost. As a result, there is no one to update the routine as systems are updated, files change, or new functions are added. In many cases the scrambling routines are obsoleted and forgotten, with the company by default returning to less secure manual processes.

The solution to these high risk, yet often misunderstood, potential security leaks is an independent data scrambling application that automatically scrambles sensitive HR data upon export from the SAP HCM database. That requirement is served by ControlPanel^GRC's HR Analyzer.

HR Analyzer™ — A More Secure Approach to SAP Data Security

Ever since sensitive HR data was taken out of locked HR file cabinets and placed on computer systems, HR data security has been a concern. Today, security issues are heightened by the much greater complexity of ERP systems, the need for an ever-wider array of people to access portions of HR databases, the proliferation of devices for accessing this information, and the younger generation's expectation that virtually all information is public domain. There has never been a greater need for automated tools to help protect sensitive HR information.

ControlPanel^GRC has stepped into the breach with HR Analyzer, a new module for SAP users to address three of the most vexing HR security needs – monitoring and protecting sensitive HR data, providing a robust viewer to non-sensitive HR files, and a built-in data scrambling routine to protect HR information used outside of production systems.

The first function of HR Analyzer is SAP HCM data usage analysis. This function monitors and reports on all infotypes and screen views of everyone accessing HR master data. This is key because the bigger data security challenge today is unauthorized viewing of sensitive HR information, not just the prevention of illegal add / change / deletes as in yesteryears. HR executives now have immediate knowledge of who is touching their data in any way so corrective actions can be taken and loopholes in security can be removed.

The second major function of HR Analyzer is enhanced employee provisioning to synchronize HR events such as hires, job changes, rate increases and terminations with SAP user IDs and passwords. Not only does this make employee data more accurate, it provides faster time to value for the personnel changes.

The third key function of HR Analyzer is data scrambling. The application automatically scrambles all sensitive HR data within SAP before it can be used for other functions like system testing or integration procedures. This ensures HR data security cannot be compromised when the sensitive data is used outside of the production system.

In summary, human resources data is some of the most highly sensitive, confidential information stored in ERP systems, yet is also the most widely used. With so many people accessing HR data from many different locations and devices, in both production and testing environments, HR data security is a much bigger challenge than ever before. ControlPanelGRC's HR Analyzer extends and complements security within SAP HCM to address these challenges – the perfect solution for today's requirements. It monitors and protects HR information usage, provides accurate one-step updates, and scrambles and protects HR data downloaded for test and back-up purposes – a simple, yet elegant solution.

*Always
Audit Ready™*