

HUMAN RESOURCE INFORMATION SYSTEMS SECURITY

AN IN-DEPTH LOOK AT SECURING YOUR HUMAN CAPITAL DATA

Companies face issues of compliance, data protection and identity theft on a daily basis. While technology is a great friend in business, it can turn into an enemy if you don't take the steps necessary to protect the security of your software systems.

As information thieves become more and more sophisticated, companies have to be increasingly vigilant to ensure that the secure private and confidential data in their databases doesn't fall into the wrong hands.

One area where businesses should focus attention is the security of their human resource information system (HRIS). These systems store confidential data—everything from salary information to social security numbers—about applicants, current and former employees, and retirees.

It's crucial that businesses analyze their HRIS to make sure it's secure and includes the many security measures and features that can help to ensure their security.

PROTECT YOUR HR INFORMATION

HR departments maintain some of the most sensitive information in any company's records, including personal employee information such as social security numbers, salaries, health data, family information, disciplinary records and so on.

It's critical to take extra security precautions to protect that information and the interests of employees and the business as a whole. In cases of security breaches, businesses are much more liable than they used to be with recent federal and state legislation such as the Sarbanes-Oxley Act of 2002 (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

Security precautions help ensure that the sensitive information residing in your system remains secure and that only the proper authorized personnel have access to it. Your HR system should include security features to do just that.

INTELLIGENT SECURITY FEATURES

It's crucial that your HRIS contains security features that prevent unauthorized users from gaining access to the sensitive and confidential information in your database.

Top-quality HR systems such as SPECTRUM Human Resource Systems Corporation's web-based iVantage® include a number of features that help protect the sensitive data contained in your HR files.

Secure Platform

A secure platform like Microsoft® SQL Server® enables the system to run at the highest level with many built-in security features. Microsoft .NET technology enables web services interoperability with enhanced performance and security. Additionally, SPECTRUM follows best practices for secure coding throughout iVantage.

User-Level Access

At the most basic level of security, iVantage requires a user name and password to access the system. Your system administrator should be able to create a user name along with a temporary password, which the user can later personalize.

Password Complexity

System administrators should be able to define their own complexity requirements for passwords using alpha, numeric and special characters. Administrators should be able to set expiration times for passwords and lock users out of the system after a predetermined number of failed logon attempts.

Role-Level Security

Role-level security defines which objects in the system a user can see. This prevents objects that users should not see from being displayed to them. For example, if a user should only see forms related to training and development, they will not see job, location or pay forms.

INTELLIGENT SECURITY FEATURES (CONTINUED)

Row-Level Security

You should be able to determine which records (rows in the database) users can see. With row-level security, managers will only see the people who report to them.

Code-Table Filtering

Code-table filtering gives only specific people access to certain system codes. A manager in the Denver location, for example, will not see salary grade codes for Chicago.

Electronic Signatures

You can use electronic signatures for approval of certain changes within the system. Electronic signatures require users to choose a series of predetermined questions to which only they would know the answers. To securely sign a document electronically, they must provide the answers to those questions.

Microsoft Windows® Authentication

Windows Authentication is an added layer of security. Users can access iVantage with their Windows passwords, therefore taking advantage of the same security protocols and password complexity requirements implemented on your corporate network.

Standard Security Protocols

A system should use standard security protocols such as secured socket layers (SSLs) to secure data in transit. SSL transparently encrypts data as it travels through your corporate intranet and the Internet.

SOX COMPLIANCE

In the wake of financial scandals, Congress enacted the Sarbanes-Oxley Act of 2002 (SOX) to protect the integrity and accuracy of financial statements issued by companies whose stock is publicly traded.

Although not designed for purposes of finance, HR systems contain information that many consider to be fundamentally related to an organization's overall financial record-keeping system and, therefore, SOX-related. Subsequently, these systems often incorporate many features that can assist an organization with SOX compliance.

Security controls—

- Controls to ensure information can't be modified without the proper approval.
- Monitoring of hiring practices to ensure you hire only qualified candidates and assign them salaries that fall within company parameters.
- Monitoring of applicant competencies to make sure they match the requirements of an open position.
- Identification of specific users and what information those users can access in iVantage.

SOX COMPLIANCE (CONTINUED)

Data storage and access—

- Single-storage source for the maintenance of employee-related data, allowing for better data controls and integrity.
- Central data repository in a Microsoft SQL Server database that you can place on a separate server from the IIS/website for additional data security.
- Storage of financial information for salary, paid time off, benefits and 401(k) contributions.
- In-depth reporting capabilities that enable you to retrieve and analyze current and historical data relevant to SOX compliance procedures.

Audit record-keeping—

- Workflow routings and approvals for an electronic trail of authorization processes for salary increases, performance reviews, time-off requests, new requisition code values, et cetera.
- Storage of all training data and training history of personnel completing SOX compliance training—automatic e-mail alerts notifying managers or employees of upcoming training.
- Tools showing customizations made and dates of updates, releases and hot fixes during system tailoring.
- Audit capabilities to determine when data was modified, who changed it, the IP address of the computer, and the date and time.
- Tracking of performance reviews, performance management and employee feedback for all departments.

PRIVACY AND HIPAA

Your HRIS should incorporate security features to ensure your organization avoids any employee privacy violations and to help you comply with the Health Insurance Portability and Accountability Act (HIPAA).

Most HR systems use an Employee ID as the primary identifier. To protect employee confidentiality, it's crucial that your system enable you to keep Employee IDs separate from social security numbers or other third-party numbers that would identify staff members.

Your HR system should also enable you to use security parameters to protect your employees' privacy. Only authorized personnel should have access to confidential information such as social security numbers or benefits information. Security roles enable only certain individuals (in HR or benefits departments, for example) to access that information.

To protect information in transit, you can tailor top-quality HR systems like iVantage to adhere to the 834 Benefit Enrollment and Maintenance Transaction Set for use in electronic data transfer through an interface.

With your HRIS, you should be able to—

- ✓ Notify the HR manager if a proposed raise is greater than company standards
- ✓ Ensure only eligible employees receive benefits
- ✓ Change organizational charts upon hire and termination
- ✓ Send e-mails to IT when someone is terminated for removal of network access
- ✓ Prevent employees from changing certain information in their own records

SECURITY TRACKING REPORTS

The ability to generate reports that detail user activity is crucial to maintaining the security of your HRIS. With these reports, you can view who is accessing the system and how they are using it.

User Access Log Reports

In iVantage, this report tracks all access or attempted access to the system by IP address of the computers used. The report provides a record of valid and invalid user names, user names entered, dates and times of attempted access, successful logons as well as logoffs—all by IP address.

User Access Log Report

In iVantage, this report provides a record of all system activity. In a separate audit database which only authorized personnel can access (typically a system administrator or executive), the system stores all the changes made to the data in iVantage. Authorized personnel can generate a report showing the changes, such as who modified a specific set of data and when.

DISASTER RECOVERY

To ensure your business will continue to run in the event of a natural or man-made disaster, it's crucial to have disaster recovery procedures in place to protect your human capital data.

Whether you host your own system or outsource application hosting to a third party such as SPECTRUM, your disaster recovery procedures should include—

- ✓ Daily backup of data and transfer to a secure offsite location
- ✓ Daily backup of transaction logs
- ✓ Weekly testing
- ✓ 24-hour monitoring
- ✓ 24-hour response
- ✓ Documentation of disaster-recovery procedures or third-party audit report
- ✓ Network recovery through alternate URLs
- ✓ Site recovery

VENDOR SECURITY TESTING

With companies placing a greater emphasis on security when selecting an HRIS, some vendors are looking to security consultants to ensure their systems are protected.

TURNING TO A SECURITY CONSULTANT

SPECTRUM contracted Security Innovation, Inc., a leading independent provider of application security services, to run a series of security and penetration tests on iVantage, as well as a full source code review for secure coding practices. The system passed.

The testing targeted areas of the system where a security risk might occur for users as well as automated attacks.

Areas tested—

- ✓ Authenticated access—Only authorized users are able to access confidential data, and only data they are allowed to see.
- ✓ Anonymous access—Until users log in, they can only see content configured explicitly by administrators.
- ✓ Non-browser access—Tested using automated tools of the same type hackers use to view and manipulate GET and POST commands or cookie content.

VENDOR SECURITY TESTING (CONTINUED)

TURNING TO A SECURITY CONSULTANT (CONTINUED)

Common website attacks used—

- ✓ SQL injection attacks—Security Innovation noted that iVantage’s parameterized queries and stored procedures harden the system against these attacks
- ✓ Cross-site scripting
- ✓ Penetration testing
- ✓ URL tampering
- ✓ Forceful browsing
- ✓ Cookie hijacking
- ✓ Network sniffing
- ✓ Security functionality
- ✓ Session hijacking
- ✓ Cross-site request forgery

A SECURITY CONSULTANT’S OPINION

“Security Innovation commends SPECTRUM for considering software security as an important and meaningful differentiator,” said Security Innovation CTO Jason Taylor. “Third-party validation is a critical step in a good security development lifecycle approach. Our security testing is designed to help SPECTRUM turn out a high-quality solution for their customers.”

“The items we tested for would allow an unauthorized user to access or tamper with mission-critical and sensitive data and escalate privileges—two extremely dangerous capabilities and, by far, the most damaging to enterprises,” said Taylor.

VENDOR BEST PRACTICES

When companies license an HRIS, they're not only selecting a product but entering into a partnership with their vendor. This is particularly true for companies whose vendor hosts their system for them. It's important to have faith in a vendor's business practices.

As a Microsoft Gold Certified Partner, SPECTRUM builds its systems on industry-standard technology that meets your HR needs, aligns with your IT department's strategic direction and integrates well with other critical business applications.

As a participant in Microsoft's Technology Adoption Program (TAP), SPECTRUM has advanced access to Microsoft's product updates and enhancements, which gives us the advantage of incorporating this knowledge into our products.

In addition to accessing Microsoft's product updates, SPECTRUM follows these practices for our hosted clients and recommends that self-hosted clients follow similar practices—

- Use SSL to encrypt data during transit.
- Monitor and apply Microsoft, SPECTRUM and third-party security patches.
- Utilize an industry-standard firewall.
- Provide adequate server administration.
- Monitor server event logs.
- Harden server security—
 - Install service packs and hot fixes.
 - Disable all unnecessary services/devices/accounts.
 - Enable logging/auditing.
 - Tighten NTFS/Registry permissions.
 - Implement time synchronization.
 - Test the system.

VENDOR BEST PRACTICES (CONTINUED)

SPECTRUM has also confirmed its high standards of system and operational reliability by achieving SAS 70 Type II and SysTrust certifications—two of industry’s most rigorous auditing certifications.

SAS 70 is the accounting industry’s measure for determining whether service providers have proper controls in place and whether they follow them. The SysTrust Seal is the accounting industry’s rigorous measure of system reliability.

While SAS 70 certifications are becoming more common in the HR industry today, few companies achieve the SysTrust Seal. To receive the seal, companies must conform to a strict framework of controls and requirements ensuring that their system is secure and available as agreed upon, that it processes transactions effectively and that it ensures the confidentiality of customer information.

FINAL THOUGHTS

Technology is a key factor in today's business, and security is a high priority. It's critical that companies examine the security measures they have in place for all of their systems, including their HR system.

When evaluating an HR system, make sure the security measures match those outlined in this paper, as do those in iVantage. Also make sure your company has a best practices methodology in place to address security issues.

SPECTRUM incorporates innovative security measures into our systems and uses best practices to do our utmost to help protect our clients' systems and ensure the security of their sensitive HR information.

THE NEXT STEP

SPECTRUM developed this white paper to help you ensure the security of your sensitive HR information.

The contents of this document derive from SPECTRUM's own creative efforts as well as research from a number of existing published sources. It is intended as an overview of the topic and is not designed as a step-by-step instruction manual.

SPECTRUM encourages individuals interested in further pursuing this topic to take advantage of information available from the Internet and other sources, including the Society for Human Resource Management (SHRM) (www.shrm.org) and the International Association for Human Resources Information Management (IHRIM) (www.ihrim.org).

Since 1984, SPECTRUM has led the HR software industry with HRIS solutions. We design the most powerful and user-friendly HR information systems on the market. Combined with our industry-leading service, we provide the ultimate HRIS experience.

Our iVantage HRIS automates everything related to HR in a single software system. In an easy-to-use web interface, iVantage enables you to track, manage and analyze data for all your employees from applicants to retirees.

Through automated workflow, you improve your efficiency and have time for other duties. With powerful reporting tools, you obtain a complete picture of your company's workforce for better strategic planning.

— SPECTRUM cannot provide legal or accounting advice regarding compliance with federal or state regulations. Companies should consult with their attorneys and auditors regarding their own compliance efforts. Each organization must determine what controls to implement for their business. —

FOR MORE INFORMATION, PLEASE CONTACT SPECTRUM AT 800.477.3287 OR VISIT OUR WEBSITE AT WWW.SPECTRUMHR.COM.