Security Well-Check for Infor/Lawson
Agenda

• About Us
• Vulnerabilities
• Other Considerations
• Other Services
• Complimentary Solutions
• Founded in 1983, Kinsey has provided software sales, implementation, support and development for 34 years.
• Lawson reseller and implementation partner since 1997.
• Lawson certified systems integrator partner.
• Lawson complementary software partner.
• Lawson’s “Go to” implementation partner for public sector.
• Provide complementary Lawson software products.
Vulnerabilities

- Securing Drill Around and Selects
- Securing Critical Fields
- Elements and Element Groups
- Resolving Conflicting Form Access
- Over-Provisioned Form Access
- Securable Types
- Self-Service Considerations
- Segregation of Duties
Securing Drill Arounds and Selects

Requirement
• Providing access to tables is required in order to see data in Drill Arounds and Selects, which allows users to select records from drop-down selection lists, and allows drilling from various screens into detailed data.

Vulnerabilities
• It’s easy to grant access to tables, but that can also allow users to drill to inappropriate data such as SSNs and executive salaries. These need to be secured at the table level.

Common Error
• Securing the Pay tab in HR11 prevents the obvious method for viewing pay, but users may still be able to drill into pay history, quarterly pay amounts, see benefits based on pay, etc.
• Improper viewing of Inventory data
• Access to Banking information
Securing Drill Arrounds and Selects

Advantages
• When you have properly secured sensitive data, then users cannot view it through screens, via experimental drilling around or by downloading data through Microsoft Add-Ins!

What we are looking for
Identify the tables supporting the form in question with drill explorer is LSA.
Securing Drill Arouneds and Selects

Then...

- Use the *Kinsey Reports* to determine who has access to the specific tables of interest (such as COMPHIST, PRRATEHIST, PAYMASTR, PRCHECK, etc. for pay amounts).

- Ensure that critical tables have rules on them to prevent inappropriate access.

- If in doubt, check the `.or (object rules)` and `.sr (screen rules)` files that contain the rules for drills and selects.
Securing Critical Fields

Vulnerabilities
• User’s may have access to sensitive PHI/PII information.
  • Can users view the Name, Address, SSN, Salary, D.O.B, Handicaps, etc., through an AGS or DME call via Portal, Ming.le, LSO, Addin, etc?
  • Frequently, users are sufficiently secured in screens, but they can drill to inappropriate data?

Common Errors/Problems
• Lack of effective communication/documentation of PII and PHI data items.
• Rash/Reactive efforts to secure these fields may make the security design top heavy with unnecessary rules. This lack of proactive planning could potentially prohibit extra-departmental staff from supplying requests for an increase in resources in a timely manor.

Our Approach
• Work with staff early to design a robust model based on all disclosed PHI and PII restriction needs.
Elements and Element Groups

Definition
While elements (ELM) are global definitions of a field, element groups (ELG) are securable objects themselves and defined by more than one element. User defined element groups are not delivered by Infor/Lawson and must be called by specific functions from forms and/or files. However, Lawson defined element groups can provide a solid foundation in the creation data level security for your business. Lawson defined element groups allow you to balance your security efforts in single point of access. Meaning, both forms and files data are secured based on the conditions of the Lawson defined element group rule.

Element example:
- Company
- Process-Level

Element Group example:
- PROCLEVEL (Lawson Defined)
  - Company
  - Process-Level
Elements and Element Groups

Vulnerabilities

• Batch Forms are the specific vulnerability (only were Lawson defined ELGs are concerned)
• If you don’t use PROCLEVEL, you have to be certain you have identified all forms and or files needing to be secured for the Role.

Common Issues

• Be careful in overlapping efforts to security data
  • Rules on the form/file to secure data vs. leveraging the ELG securable object to secure data.
  • Streamline (minimize) data level rules – You do not want to overlap ELG rules of the same type.
  • Not understanding the system code and element dependencies.

Advantages

• Using Lawson delivered ELG in your security strategy is the most efficient way to secure data for online, batch and file access.
Resolving Conflicting Form Access

**Definition**
- The common problem of a user having access to a form through more than one Role or Security Class.

**Diagram**
- User
- AP Manager
- AP Setup
- AP Proc.
- VendorRO
- AP11.1
- AP00.1
- AP10.1 ALL-ACCESS
- AP10.1 ALL-INQUIRY
Resolving Conflicting Form Access

Vulnerabilities
• Potential for users to have more functionality on a form than desired (i.e. A,C,D versus Inquiry only)

Common Issues
• Not realizing that a user has access to a form through more than one path.
• Not understanding how Lawson resolves “least restrictive” access to an object.
• Attempting to change access for one user snowballs into many changes affecting lots of users. Small changes quickly become impossible to complete.
Resolving Conflicting Form Access

Our Process/Solution

• We will identify the duplicates, determine which are the most crucial, and work with your team to resolve them.
Over-Provisioned Form Access

Vulnerabilities
• User’s may have access to forms that violate SoD policies or with critical information not related to their job.

Common Issues
• Not having a good understanding of exactly what forms a user requires to do their job.
• Your technical staff has WAY too much access (according to auditors). What can you do?
  • We’ll configure Kinsey Activity Monitor reports for auditors showing exactly which screens tech users have been using to view or change data, including whether changes were made at all.
  • We will help create a configuration that prevents tech users from changing data without following your proper methodology (user involvement, documentation).
Our Approach

- We’ll use Kinsey Reports to determine exactly what users have access to and how to quickly restrict that access.
- Did they go “off the rails” and use inappropriate screens?
- We’ll show how to use Kinsey’s Activity Monitor to quickly determine what screens they used and if they simply inquired or made changes.
Over-Provisioned Form Access

Reporting
• User Activity
• User Activity versus Security
Object Type - Securable Types

**Definition**
- Provides **global** access to forms or files.

**Vulnerabilities**
- Overrides any user specific object rule for Form (online and batch) and Files.
- Improper provisioning of Securable Type object inadvertently provides too much access.
Common Misunderstandings
• Not realizing that Securable Types object rules have been assigned.
• That Data level rules will still be adhered to.

Advantages
• Can quickly provide full access to someone who needs it (i.e. Security Admin)

What you need to check in Security Administrator
• Validate access to securable type of TYP.
Object Type - Securable Types

Reporting

• User All Objects Report
• Role – Security Class All Object Report
• Security Class All Object Report
ESS/MSS Considerations

Definition
• ESS/MSS – Employee and Manager Self Service are a set of “self evident” applications or bookmarks that allow you to inquire or update HR, LP, BN, PA, or PR data in Lawson as the employee identified on the Employee Service.

Vulnerabilities
• The risks of not setting the EMG rules and corresponding forms up correctly is exposure of PII/PHI or employment related data to users other than themselves.
ESS/MSS Considerations

Common Errors

• Leaving HR Data Item or HR Record Security active.
• Supplying ALL USERS a ENV Identity. Not necessary for ONLINE users.
• Not setting up your Privileged User/Identity correctly.
• Not understanding the symbiotic relationship between the user defined EMSS ELG and EMSS forms/files.
• Unnecessarily leaving batch forms in your EMSS security class.
• Not communicating actual tasks your organization uses in EMSS.
• Not testing customizations created for EMSS or evaluating where antiquated technology can be retired.
EMSS Considerations

Our Process

• Review your EMSS task and tailor the security class(es) to your organization’s needs.
• Review the EMSS security class for the appropriate conditional rules.
• Review your Privileged Users and User Setups.
• Review EMSS forms that may provide access to sensitive data (outside of the required access of EMSS). i.e. PA52.x
• Review the drill right of the Manager. What PHI or PII data is accessible to them for their direct reports (outside of the scope of their managerial tasks).
• Review your current setup for HR Record level or Data level security setup within the HR application
Segregation of Duties

Definition
• Segregation of Duties (SoD) validates that you have the proper checks and balances in place to prevent fraudulent activity.

Vulnerabilities
• Exposure to a number inappropriate financial transactions including check processing, asset retirement, closing procedures, inventory transactions or journal transactions.

Common Issue
• The process of developing a list of policies and appropriate rules and then checking user security against those rules can be a daunting task. Most customer’s find it very difficult to even start this process manually.
• Validating user security against those rules.
Segregation of Duties

Our Process

• We start by reviewing with your team the 240 policies delivered with the application.
  Asset Management, Cash Management, Closing, Inventory, Order Entry, Payables, Receivables, and Payroll
• We then add any of your policies to our library.
• Using over 2,200 rules our SoD report will identify any user that violates a policy and the reason for the violation.
• Identify the users and policies that present the highest degree of risk.
• Modify security to mitigate the risk.
Segregation of Duties

Our Policies and Reports
Remediation Process

- By merging user activity with the violation results we can identity the policies that present the most immediate risk.

*Requires activation of Activity Monitor*
Other Considerations

• Building Inquiry-only Roles
• Cleaning Up Menu Access and Invoked Programs
• Eliminating Duplicate Roles and Security Classes
• Standardizing Roles
• Synchronizing Your Test and Production Environments
Building Inquiry-only Roles

Definition
• The ability to easily grant inquiry-only access to all screens and all reports.

Vulnerabilities
• Users are often provided more access than they need to perform their day to day task. Inquiry only Roles resolve potential SoD violations and can prevent fraudulent transactions.

Common Errors/Problems
• Some Roles or Security Classes may have names such as APInquiry, but include update-access to certain forms. This is misleading, or even dangerous.
Building Inquiry-only Roles

Advantages
• This lets you confidently give access to auditors or others with no concerns about them being able to make any changes in the system.

Options
• Manually build inquiry-only configurations.
• Export Lawson Security Roles or Security Classes, adjust the XML to use ALL_INQUIRES in the place of A,C,D,I,N,P and load into new Roles/SecClasses
• Kinsey has utilities that allow us to build inquiry-only configurations that match your environment, including custom programs.
Cleaning up Menu Access and Invoked Programs

Why we do this

• Menu’s and Invoked Programs tend to land in various Security Classes and create a “can’t see the forest for the trees” situation. It’s much cleaner and easier to control this with a well-organized solution.

Common Problems

• Not having proper access to a critical invoked program can impact your job related task.

Our Process

• Review and cleanup the usual mishmash of Invoked Program access.
• Clean up menu token access.
• Use innovative concepts to eliminate the forest of SysCodes and Programs that make the true screens harder to view and analyze.
Eliminating Duplicate Roles & Security Classes

Why we do this
• Makes the security model easier to maintain and less prone to error.

Vulnerabilities
• Easy to lose track of all the paths to a critical object. (i.e. Employee Master HR11.x)

Our Process
• Eliminate the duplicates which always cause maintenance nightmares.
• Compare and consolidate Roles and Security Classes.
Eliminating Duplicate Roles & Security Classes

Reports
Role & Security Class Comparisons
Why we do this
• Makes the security model easier to maintain and less prone to error.

Our Recommendation
Put all of the standard Roles...

BatchRole; LawsonQueryToolsRole; ProcessFlowRole; PortalBookmarkAdminRole; Data Area Access Role

...into ONE single Role named something like:

• 1KinseyALL (starting with 1 so it always sorts to the top to be quickly assigned to users).
• Give 1KinseyALL to every new/changed user and forget about those other Roles.
Typical Setup

Optional Setup

Standardizing Roles
Typical Setup

- GLIFInquiry
- TXMaintenance
- ACAccountant
- BatchRole
- DataAreaAccess Prod
- LawsonQueryTools Role
- ProcessFlowRole
- PortalBookmark AdminRole
- BatchRoleClass
- DataAreaClass
- QueryToolClass
- ProcessClass
- BookmarkClass

Optional Setup

- GLIFInquiry
- TXMaintenance
- ACAccountant
- 1clientnameRole
- BatchRoleClass
- DataAreaClass
- QueryToolClass
- ProcessClass
- BookmarkClass

Standardizing Roles

Other Considerations

Security Well-Check
**Why it’s important**
Many companies have moved well-tested patches or modifications from TEST to PROD, only to have them fail in PROD! Now what do you do?

- You have crucial tests underway in TEST – you can’t risk those by simply copying PROD security onto TEST.
- And you have security rules in TEST that you’re testing – you can’t lose those!
- You could endeavor to ferret out everything that’s different, if you only had lots of time for that.

**Our Solution**
- We'll do a comprehensive comparison of security between the TEST and PROD, determine the significance of differences, and synchronize the two in the most effective manner.
Our Reports

- Environment and Profile Security Comparisons

Synchronizing your Environments
• Reviewing the Organization’s Onboarding Process and Automating Procedures.
• Landmark Security Review
• Environment Identities - what is required based on Online or Batch user?
• What are your Privileged Identities and when are they used?
• PHI/PII Security Review
• Demonstrate features of ISS and assist with the sync.
• Any other issues you are currently experiencing.
## Complimentary Solutions

**Security Reporting**
- User
- Role
- Security Class
- Usage Comparison

**SOD Reporting**
- 200+ Prebuilt Policies
- Violation Reports
- Email Notifications

**Security Auditing**
- Audit all object changes
- Email Notifications

**Transaction Auditing**
- Selectively audit over 6500 Lawson Forms

**Activity Monitor**
- Audit
- Security Tuning
- Unauthorized Access

**SOD Remediation**
- Risk Analysis Grid
- Security Modeling

**Security Modeling**
- Build What-if scenarios for Users, Roles, Forms

**Landmark Reporting**
- Actor
- Role
- Security Class
- Lawson LPL Detail
Security Review
Our team of security consultants will review your existing configuration and make recommendations on potential changes.

Security Consulting
Our analysis will include a Statement of Work for our consultants to assist you with implementing any changes.

Applications
During the review process you will have full use of Kinsey’s Security and SoD Reporting tools at no charge.
Contact Us

Email: g.henson@kinsey.com
Call: 757-621-8236
Website: www.kinsey.com

Thank you for attending!

We hope you found it helpful!