A Security Checklist for ERP Implementations

A study of ERP security issues produced a checklist that shows institutions what to look for while letting vendors know what campuses consider important

By **Joy R. Hughes** and **Robert Beer**

Enterprise resource planning (ERP) systems are often the single most expensive software system that a CIO will ever implement. When all costs are considered—hardware, software, network upgrades, staff time, training, and consultants—an ERP system can cost $10–$50 million to implement. Millions of dollars can be spent just to provide the same level of management information that the hundreds of reports designed to work with the old system provided. Unsuccessful implementations and huge cost overruns are not uncommon and can lead to legal action by the school against the ERP vendor or consultants when the project fails during implementation. Although lawsuits are uncommon, they bring considerable notoriety to an institution and add strength to the mythology of the career-ending ERP implementation.

New Systems, New Challenges

In recent years, the situation has become worse for several reasons. Because they replaced labor-intensive processes, initial ERP implementations at many institutions resulted in dramatically improved services as well as cost savings. Today, an ERP will likely replace an existing ERP that has been customized over the years to meet specific institutional needs. For example, the institution might have modified the system to provide the data needed by research faculty to manage their grants, or modified the waitlist program to automatically enroll students in a course when a seat becomes available. If a new system is implemented that doesn't include these functions, the research faculty will be furious when they find they have lost their management tools, and the institutional enrollment strategies will no longer be reliable because the new waitlist program functions differently.

Rather than realizing savings in staff time, implementing a new ERP will probably require more staff because institutional processes and procedures were modified to best fit the old ERP. It will take years before these processes can be adapted to the new ERP or the new ERP customized to fit the organiza-

tion's special needs. Moreover, even as a new ERP adds new features, other legacy features will be lost. For example, the old ERP might allow research faculty to track expenditures at a fine level, while the rest of the institution tracks at a grosser level, thus meeting the needs of both groups. Or the old ERP might have been optimized for efficient processing of financial aid awards, whereas the new ERP requires staff to labor through many screens in order to process an award.

Another significant problem area when implementing a new ERP is the security of institutional data. An ERP system being replaced today probably runs on a huge machine, often a mainframe or super server, and access to the data in the system is restricted to the central IT staff. In many cases, if an academic department needs information, it requests a hard copy report that is delivered in the campus mail. Some institutions using older ERPs have implemented data warehouses to provide data from the ERP. Frequently, however, only "power users" know how to use the data warehouse, and they often can only generate reports, not download the data. New ERPs are designed to allow many members of the university community to see and change data and produce reports. In this new environment, it has become quite challenging to ensure that only those with a need to know have access to the data.

A changing regulatory climate adds another layer to the difficulty of procuring a new ERP system. Some states have issued regulations requiring the top security professional in a state college or university to certify that software is secure before the institution may procure it. Even in the absence of such legislation, some institutions have independently instituted this practice.

Security Concerns

The EDUCAUSE/Internet2 Computer and Network Security Task Force consulted with IT security professionals on campus about concerns with the current state of security in ERP systems. From these conversations, it was clear that security issues generally fell into one of two areas:

Members of the task force wondered if ERPs in use on the majority of campuses today could pass a stringent security review

- It has become extremely difficult to understand how to securely configure an ERP system and the myriad of products purchased to integrate with it—products like report generators, data warehouses, learning management systems, imaging systems, portals, and others.
- The overhead of managing access and authorization roles—for both the ERP and third-party software integrated with the ERP—is huge. Institutions said they had backed off from using role-based security because the overhead of managing it was just too high. For example, rather than setting up fine-grained role access so that only biology faculty can see the records of biology majors, an institution might set up one role called "faculty" and allow all faculty to see the records of all students, thus increasing the opportunity for data misuse and violations of data privacy.

Given the concerns of security professionals on campus and the growing number of policies requiring certification before an ERP system can be purchased, members of the task force wondered if ERPs in use on the majority of campuses today could pass a stringent security review. The task force proposed developing a checklist of effective practices for ERP security. Such a checklist would provide guidance to ERP vendors about the security features that are most important to higher education and to higher education security and administrative systems professionals for both the product-evaluation and system-configuration phases of implementing an ERP.

Developing the Checklist

Members of the task force consulted with security professionals, managers of administrative systems, IT auditors, and others to identify elements that should be included in the checklist. To assist their efforts, the task force approached SunGard Higher Education, which currently has the largest share of the higher education ERP market. SunGard agreed to work with the task force and arranged for a third-party research firm to develop a focus group protocol, which was administered to several focus groups of SunGard customers.

Participants in the focus groups included directors of administrative systems and CIOs. Later, the information gathered in the focus groups was tested with higher education security officers. Although this last group understandably expressed stronger concern about the security features of ERP systems, there was considerable overlap among all groups surveyed for many of the responses. These concerns included:

- Complexity in configuring and managing ERP systems, which was made more challenging by a lack of sufficient information from vendors
- Weak passwords and relative insecurity of reporting tools
- Degradation of performance when using higher-security settings and procedures, such as enabling encryption and audit trails
- Bundling of proprietary identity management (IdM) systems in an ERP system, rather than offering ERPs that

use open standards and can interoperate with any enterprise IdM system the institution chooses

The task force used responses from the focus groups to draft a checklist of ERP security issues. This initial draft was limited, however, because all input had come from users of the SunGard system and because the checklist did not prioritize the issues. To gain wider input, the task force sought information from campuses that used other products. Through similar questionnaires, data were collected from users of PeopleSoft, Datatel, and Jenzabar ERP systems. The task force found remarkable consistency among responses. That is, users of each of the ERP systems covered by the survey tended to report the same security shortcomings as every other campus that used the same ERP system.

To gather information about the relative priority of the items on the checklist, the task force questioned attendees of a session on ERP security at the 2007 EDUCAUSE Security Professionals Conference. Attendees at that session were given the checklist and asked, "If your school were about to buy an ERP system, and you—as the security professional—were asked to approve the purchase, which of the items in the list would be deal killers?"

In its final form, the checklist (below) includes 38 items, of which 19 were identified as deal killers. Comparing the checklist to the responses from the various focus groups shows that every ERP system widely used in higher education today has security flaws considered deal killers and would likely be rejected by a knowledgeable security officer asked to evaluate it. Because more and more states are requiring institutions to vet software for security flaws prior to procurement, we may soon see that state institutions will be prohibited from purchasing a new ERP.

The Checklist

The task force organized the checklist into four subsections, as outlined below. Within each subsection, the deal killers are listed first, as the "must-have" features, followed by the desired features.

Questions for Similar Institutions

For the following criteria, it is essential that the ERP vendor provide the names of institutions that are similar to yours in size and complexity. You should then ask the following questions regarding ERP features:

Must-Have Features

- Have you found that role-based access is sufficiently easy to manage that your institution is able to specify the number of different roles needed to ensure that only those people who have a "need to know" actually have access, rather than deciding to accept the risk of using fewer and broader roles?
- Does your auditor consider the workflow diagrams and other process documentation provided by the vendor to be sufficient to conduct an efficient and productive audit of relevant processes?

Desired Features

- Have you found that you can encrypt as many fields as desired without degrading performance?
- Have you found that you can put audit trails on as many fields as desired without degrading performance?
- Do you feel that creating duplicate records during data entry is not so easy as to cause concern about the integrity of the data?
- Have you found that the systems the vendor provides to avoid the creation of duplicate records work well and are not so cumbersome or so detrimental to system performance that your institution declined to use them?
- Do you find it relatively easy to deactivate access to the system for a user?

Sample Work Products and Other Documentation

The vendor should provide sample work products or other documentation that you can examine in order to answer the following questions:

Must-Have Features

- Is there a comprehensible report that articulates the security implications of giving a user access to fields/tables/forms?
- Is role-based access sufficiently granular that one can be sure that only those with a need to access certain data will be able to access that data?

Desired Features

- Is each standardized data field adequately documented in a data dictionary?
- Which data fields have table lookups?
- What combinations of fields have validity rules controlling data entry?
- What reconciliation and exception reports are provided?
- What reports are provided to make it easy to locate duplicate records?
- What reports are provided that show who has access to processes that involve sensitive data?

Vendor Security Certification

You should require the vendor to respond to these items in writing:

Must-Have Features

- The ERP system requires strong passwords.
- There is a low overhead and secure method to change passwords.
- Stored passwords are encrypted.
- There are no features of the ERP that require that users, no matter what their role, be given access to the underlying database.
- The ID is not the SSN.
- Roles can be tied to position categories.
- Default roles can be established.
- Roles can be established that allow a user to process sensitive data in the ERP but restrict that user from downloading the data.
- All data fields that are required by federal law to be protected come with encryption enabled.
- All data fields that are required by federal law to be protected come with auditing enabled.
- Data fields can be encrypted at the database level as well as at the form or table level.
- Reports are generated that show who has requested data exports that include sensitive data, such as SSNs, credit card numbers, and so forth.

Desired Features

- Critical processes (payroll, grades) can be run first in audit mode.
- The institution can specify additional fields to have table lookups.
- The institution can specify additional fields to be encrypted.
- The institution can specify additional fields to have audit trails.
- The system prevents the creation of duplicate records during batch transactions.

Integrated Third-Party Products

ERP vendors often talk about integrated solutions, which comprise the vendor's ERP modules plus a set of third-party products that the vendor advertises as working well with the ERP—products such as portals, imaging systems, and learning management systems. Unfortunately, sometimes the purported "integration" does not work well, particularly when it comes to maintaining security. Here are some questions to which vendors should respond in writing:

Must-Have Features

- Is there an easy-to-use tool available from the vendor or a trusted third party that allows one to see the access that has been provided a user with respect to the fields/tables/forms in the ERP, its underlying database, and integrated third-party products and reporting tools?
- Is there an easy-to-use tool available from the vendor or a trusted third party that facilitates providing access to and deactivation from integrated third-party products and reporting tools when one provides access to or deactivation from the ERP?
- Will the ERP and the integrated third-party systems work well with the institution's IdM system? Specifically, the HR and student systems should feed the IdM; the IdM's database should manage the associated ERP roles; and the ERP and the integrated systems should have password-change policies and timelines that can be subordinated to and controlled by the IdM.

Desired Features

- Is security controlled at the database level, or must each application configure and control its own security?
- Do the integrated products have a role-based architecture that is consistent with the ERP? That is, if an ERP role disallows the user from seeing grades, would the integrated reporting tool also disallow the user from querying grades?
- When the institution uses the reporting system recommended by the ERP vendor, will sensitive data be encrypted as it passes from the central system to desktops, departmental servers, and so forth?

Recommendations

The task force shared the checklist and the results of this study at the EDUCAUSE Enterprise Technology Conference in May 2007. Most of the attendees manage large enterprise systems, including ERPs, at their home institutions, and they recommended that institutions develop a comprehensive enterprise approach to security prior to ERP procurement. This enterprise approach, they noted, should be designed to include the ERP and its associated products, as well as other current (and future) enterprise systems such as course management, e-mail, building-access management, and the myriad other systems that have assumed enterprise-level importance.

Almost three-fourths of the deal killers identified by higher education security professionals involve security flaws in the areas of authentication and authorization, role and privilege management, and passwords and password management. These are all topics addressed by the NSF-funded middleware project of Internet2 (http://middleware.internet2.edu). Some IdM systems designed to work across all enterprise-level systems have adopted middleware standards. These enterprise-level IdM systems (E-IdMs) hold the key to addressing most of the security flaws identified as deal killers.

The task force recommends that any higher education institution issuing a request for proposal (RFP) for a new ERP include a requirement that the vendor explain how the ERP will work with the institution's E-IdM to obviate the security flaws in the ERP. If the institution does not have an E-IdM, the RFP should require the vendor to propose an open standards E-IdM that includes the core Internet 2 middleware services for E-IdMs. The ERP vendor's response to the RFP should fully detail the costs associated with implementing the E-IdM along with the ERP and its associated products.

The remaining one-fourth of the deal killers involve security flaws that could be remediated either by vendors' working with institutions in the pre-implementation stage to create documentation, workarounds, and interfaces or, preferably, by vendors' building these into the standard ERP package. The task force recommends that all RFPs for new ERPs require that the vendor either certify that it has remediated these security flaws or cost out any additional steps needed to address them.

The security checklist provided here can assist institutions facing the challenge of choosing or implementing an ERP system that will securely manage institutional data. The must-have and desired features list quickly points out ERP product security shortcomings. The more items on the checklist that an ERP system addresses, the better it will serve the needs of the higher education community. Security is not solely the vendor's responsibility, however. Institutional implementation and configuration play a huge role in an ERP system. Institutions need to have a comprehensive security plan in place before the ERP implementation begins. The institution and the vendor need to work closely to ensure that ERP security considerations are understood and addressed, resulting in an ERP implementation that reliably meets the project's goals while effectively safeguarding the vast amounts of sensitive information contained in such systems.

Joy R. Hughes (jhughes@gmu.edu) is Vice President for Information Technology and CIO at George Mason University and is Co-Chair of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Robert Beer (r-beer@onu.edu) is Director of Academic Computer Users Services at Ohio Northern University.