Educational Resource Systems Risk Assessment

Memorandum

To:	Jennifer Pereyra Steve Medina	**Date:**	20 May 2008
From:	Blair Meiser Paul Lusardi	**cc:**	Erica Abramson Hattie McKelvey
Subject:	Educational Resource Systems Risk Assessment		

The J&J Information Asset Protection Policies require that we perform a business partner risk assessment of all suppliers who have access to J&J business critical information, or who have requested access to JJNET. The policies also require periodic reassessment of those same suppliers to ensure that they continue to protect our business critical information.

The purpose of this document is to convey the findings of a business partner risk assessment of Educational Resource Systems (ERS) performed on 20 May 2008.

Paul Lusardi performed the assessment. Based on the business partner risk assessment questionnaire answers and clarifications provided during the site visit at the company's facilities in Red Bank, NJ, there are no risks or issues that would preclude J&J from continuing to grant LPA access to ERS as they meet J&J standards for information security. More detailed information is presented in the report that follows.

If you have any questions, please contact either Blair at 908-541-4633 or Paul at 908-541-4174.

COMPANY Risk Assessment

Company Background
According to their website www.educationalresource.com:

> **Educational Resource Systems, Inc.** is a medical education company offering creative solutions for sales training and medical communications.
>
> With offices in New York and New Jersey, ERS personnel have produced over 750 training programs for pharmaceutical products and devices in virtually every therapeutic area. Our software training programmers pioneered both sales training and value-added CME programs on laptop computers using state-of-the-art computer graphics and animation.
>
> In addition, our editorial, technical, and computer staff is expert in development and application of interactive multimedia programs employing video, audio, computer-generated graphics, and animation. These programs range from CD-ROM to web-based applications.
>
> ERS is actively involved in the various issues of Health Economics. In the U.S., our company is developing generic programs to guide field representatives through the many considerations imposed by Managed Care. Programs have also been developed for field sales managers and product managers in areas of Strategic Planning to ensure company-wide consistency of organization and execution.

The Risk Assessment

SUMMARY OF FINDINGS
The answers on the Risk Assessment and the clarifications provided by ERS at the meeting at the company facilities in Red Bank, NJ identified no risks or issues that would necessitate corrections or otherwise suspend the LPA access that ERS has to JJNET.

GENERAL FINDING

ANTIVIRUS AND MALICIOUS SOFTWARE PROTECTION - Compliant
ERS uses McAfee solutions for anti-virus and email and attachment scanning. ERS utilizes McAfee off-the-shelf anti-spyware, which is run on an as-needed basis. This company has a small number of employees (35), over half of whom use Mac computers, which makes this acceptable. Windows software firewall is also utilized on company machines.

PERSONNEL SECURITY – Compliant
Personnel are subject to educational and past employment checks, as well as a criminal background check. New employees are required to take informal information security training as part of the on-boarding process.

INFORMATION VALUATION AND PROTECTION – Compliant
Customer information is encrypted via 128 bit SSL when transmitted over public networks. Email is encrypted at the server, which is housed at the co-location (U2 Networks, based in Texas).

PASSWORD AND PIN SECURITY – Compliant
ERS employs a minimum "6+3" password strength/complexity (minimum of 6 characters, plus three of the following character sets: upper case, lower case, numeric, special character). Passwords are force-changed every 90 days, and the previous 3 iterations are not allowed. New passwords are only delivered via telephone or in person.

ACCESS CONTROL GATEWAY SECURITY – Compliant
The co-location utilizes a Cisco ASA hardware firewall, and locally a Firebox hardware firewall is employed. Local UPS has a 5-8 minute battery back up.

PORTABLE COMPUTING DEVICE SECURITY – Compliant
Remote users are disconnected after 30 minutes of idle time. The loss of any customer information will be reported immediately to the primary J&J customer.

CRYPTOGRAPHY - Compliant
Cryptography is adequate, and conforms to all J&J standards and policies.

SYSTEM AND APPLICATION DEVELOPMENT SECURITY – Compliant
ERS utilizes a formal SDLC methodology, and conforms to all J&J standards and policies.

SECURITY INCIDENT REPORTING – Compliant
Security monitoring is performed both by the co-location, and locally in-house. Security incidents are by policy reported to the J&J main contact as soon as the incident is confirmed.

INTRUSION DETECTION – Compliant
Intrusion detection is host-based, and handled by McAfee Host Intrusion Prevention. Security breaches will be reported to the main J&J contact, as mandated by policy.

GOVERNMENT REGULATION COMPLIANCE – Compliant
Government regulation compliance is adequate and conforms to all J&J standards and policies.

CONTINUITY OF BUSINESS AND DISASTER RECOVERY – Compliant
Business Continuity and Disaster Recovery plans are formal and enterprise-based. Fireproof safes in 2 remote offices handle off-site storage of vital documents. The most recent test of the BC/DR plan was performed in January 2008.

PHYSICAL SECURITY OF INFORMATION ASSETS – Compliant
Visitors are logged in when entering. No employees are required to wear ID badges, but with only 35 employees, any unauthorized persons would be immediately noticed. Local servers are in a locked cage in the office. Only the IT manager and the owner have keys to the cage. The most recent test of the local UPS was performed in April 2008. Customer data stored on magnetic media are wiped clean prior to disposal with DoD-compliant software.

NETWORKING AND COMPUTING RESOURCES ACCESS SECURITY – Compliant
Networking and computing resources access security is adequate and conforms to all J&J standards and policies.

INFORMATION SYSTEM ADMINISTRATION AND MANAGEMENT SECURITY - Compliant
Security patches are tested in a staging environment prior to being deployed to production. New unused accounts are disabled after 30 days, inactive accounts are disabled after 45 days, and disabled accounts are deleted after 90 days. Incremental back ups are performed daily, and full back ups weekly. Back up media is encrypted in storage. The most recent data restoration test was performed in January 2008. Paper media are shredded upon disposal.

WIRELESS SECURITY – Compliant
ERS employs wireless technology. Ad-hoc networks are prohibited, and scanning is performed on an as-needed basis, as is scanning for rogue devices.

ELECTRONIC MEETING AND COLLABORATION SECURITY – Compliant
Electronic meeting and collaboration security is adequate and conforms to all J&J standards and policies.

BIOMETRIC TECHNOLOGY – Compliant
Biometric technology is not employed at ERS.

CONCLUSION
Educational Resource Systems is compliant with all J&J IAPPs. There are no risks or issues that would preclude J&J from continuing to provide LPA to ERS.

RECOMMENDATIONS
None