CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

Despite the fact that credit unions are continuously implementing more sophisticated safeguards, hackers are some of the most adaptive people out in the cyber world. They are constantly finding new ways to penetrate systems. There isn't a one size fits all answer for what is the best security strategy. The best things that credit unions can do is to constantly ensure that they are in full compliance with the comprehensive federal data protection standards. Paying close (and when I say close, I mean annoyingly detailed) attention to the standards imposed by Gramm-Leach-Bliley should be of highest priority.

Because OnBase captures and stores data and documents, security has to be top of mind as we develop, configure and deploy the solution. Credit unions have complete control of their OnBase content to ensure that appropriate document access and privileges within the application are defined down to a very granular level. OnBase also allows the administrators / IT to protect the system against unauthorized access with tools such as data / document encryption, protection from directory traversal attacks, and protection of passwords in the OnBase database using sophisticated hashing algorithms.

In terms of auditors and examiners, they tend to focus on a couple of key areas when it comes to ECM and the overall security of the data and documents contained in the system. The first area of focus is on access control. The security model used in the OnBase system provides for the segregation of data between users, as well as the ability to limit the product functionality available for each user. User Groups and Rights provides for the assignment or restriction of basic and advanced OnBase features. Privileges can be assigned in a granular manner in OnBase. This control is entirely in the hands of the administrators. Assuming that users' privileges are appropriately configured within OnBase, auditors are typically satisfied.

The other area that auditors tend to focus on revolve around the more defined security standards and policies outlined by Graham-Leach-Bliley, PCI Standards, etc. In most cases, the focus is on the security of the data itself. Encrypting both the documents at rest as well as the meta data using AES-256 bit encryption provides an additional layer of security for content stored in OnBase. Sensitive alphanumeric keywords are stored in the database in an encrypted format, with access to view full or partial values granted to authorized users. Documents are automatically encrypted as they are imported into OnBase, becoming indecipherable when retrieved outside of the system. Even within OnBase, these files are accessible only to permissioned users, further decreasing risk of exposure. Risk of exposing private data is eliminated and compliance with industry standards such as the Payment Card Industry (PCI) Data Security Standard (DSS) is enhanced. Encrypted Alpha Keywords provides the necessary tools to securely store sensitive data digitally — preventing costly security breaches and keeping you and your data safe.

Steve Comer
Manager, Financial Services

OnBase by Hyland

Contact Info

www.onbase.com
440-788-5810

Steve Comer is the credit union industry manager at Hyland Software, Inc., the developers of OnBase®. An award-winning suite of enterprise content management (ECM) solutions, OnBase has a proven record of solving problems resulting from time consuming, costly and error plagued manual tasks. As the credit union industry manager, Comer is responsible for developing sales, marketing, and product strategies that will help credit unions realize faster ROI, increase process efficiencies, and provide enhanced member service through the use of OnBase. He also cultivates and manages both new and existing partner relationships with other vendors to bring added value to CUs.