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

Here are three key defenses credit unions can actively pursue as best practices that will better safeguard members and their personal financial information:

1) Do not use “old” technology. Keep all systems and technology platforms up to date and current with necessary patches. The latest versions of IT infrastructure components – firewalls, servers and Web browsers to name a few – are designed to remain a step ahead of various threats. While it may seem too frequent, unnecessary or too expensive, falling behind on software release versions because of competing projects or lack of resources could increase your risk of exposure.

2) Ensure vendor applications are also updated and “modern.” Your vendor partners dedicate a lot of effort, time and cost toward releasing frequent product and service updates. Credit unions need to take advantage of their strategic relationships and keep up with these latest releases, ensuring systems run efficiently and properly. Additionally, closely evaluate the security history of new vendors you are considering as a part of the due diligence process. Pay as much attention to the platform components and security commitments as you do the feature functionality of the systems.

3) Make electronic transactions happen. They eliminate paper-associated risks, but also provide value in today’s electronic processing environment in the form of efficiency, cost savings and member convenience. Make sure that the systems you are using for electronic processing are also secure, current in technology infrastructure and that the vendor has a strong commitment to information protection and security. For example, data within systems in process or at rest should be encrypted at all times.

In terms of helping to mitigate data breaches, all of IMM’s solutions maintain the highest standards of modern architecture and security design. The data contained in any electronic transaction passing through our software is encrypted. For a data breach to occur at a credit union, not only would the hacker have to get into the institution’s infrastructure first, but then would also need to gain access into our repository. Should that ever happen, inside that repository, data is fully encrypted – meaning an incredible amount of work and effort on the attacker’s part without the reward of getting anything for it.

Electronic processes overall provide credit unions with a boost in their security measures. In the case of our eSignature technology, any completed documents have the added protection of a PKI wrapper that maintains ongoing integrity of the document contents and signatures. This means that in the event of a data breach, anyone attempting to alter the content or signature would break the tamper-evident seal and visually compromise the document. The document tamper evident seals, industry standard methods of signer authentication and comprehensive audit trails within our eSignature platforms make each transaction legally enforceable. eSignatures have been legally acceptable for almost 15 years now and all IMM solutions are built in accordance with standards outlined in legislative acts, such as UETA and ESIGN.

Our workflow technology is a compliance officer’s dream in the way it allows defined, automated process flows regulate and control a credit union’s operational environment. Credit unions can limit actions and decisions to designated employees while tracking and documenting all activities and employee actions in the transaction audit trail. Presenting this type of electronic record to any examiner provides evidence of not only compliant operations, but also of measures to protect information and prevent fraud.

Finally, credit unions need to investigate any partner’s certifications. IMM has invested the time and resources to be compliant with regulatory requirements as well as uphold SSAE-16 SOC 1 & 2 designations and PCI Certification.

John A. Levy
EVP and Co-Founder

IMM

Contact Info

www.immonline.com
Phone: 800.836.4750

John A. Levy is the executive vice president of IMM, a company specializing in paperless technologies that improve a financial institution's transaction process by automating the space between its core host system and imaging backend, including digitized signatures in-branch or remotely. His core responsibilities at IMM encompass overseeing the day-to-day operations of the sales, support, development, quality assurance and design teams. Levy's vision for IMM is to continue to be the leader in delivering quality software to the financial industry that increases productivity and reduces operating costs by streamlining the typically paper-centric financial institution output processes. Teamwork, excellent service and the development of a strong infrastructure are the foundation of Levy's daily operating style.