

Protecting Member Data at Rest and in Motion

The information that resides in and flows to and from your credit union is one of the single biggest sources of risk to your institution. Vast amounts of sensitive data, a lack of education amongst unsuspecting victims, and the creative energy and juices flowing from the minds of cyber criminals can be a recipe for disaster. Detailed risk management policies and risk mitigation practices are critical to manage against the risk to your institution's reputation.

Regardless of the number of times we hear about the various schemes employed by cyber criminals, their crimes continue, often escalating during peak transaction periods. The hackers will continue their focus; therefore we must continue our due diligence, vigilance and be thoughtful, and yes fearful, of the continued scams.

Perimeter security plays a role in an overall security plan. In addition to firewalls, intrusion detection systems, log reviews, security patches and network equipment, process plays an important role in shielding your credit union from the outside world.

Internal security protects from the inside out - detailing who is allowed to do what; who grants that authority - and the authentication and ongoing monitoring of the various "who's" to prevent malicious activity. Inside security requires the same type of processes as perimeter security - along with routine, frequent audits to ensure that only specified staff members have access to the appropriate data.

To make the management of perimeter and endpoint security more efficient, Harland Financial Solutions' applications support Single Sign On, which enables credit unions to centrally manage authentication and authentication policies to ensure consistency. Our applications each add their own definition of rights, based on the access group the authenticated user enters, controlling which activities they are allowed to perform within the application. In addition, logging capabilities monitor authorized activities for suspicious behavior.

Organizations of all sizes are exploring encryption because of the real threat of losing data or having it stolen. Hackers work hard to create new ways to access members' non-public information (NPI). Harland Financial Solutions' UltraData® Enterprise core system and backup files encrypt all data "in motion" as well as authentication data "at rest". As a result, access to that data outside of the authenticated and monitored application itself is prevented. Additionally, multi-factor authentication, as recommended by the FFIEC, and fraud monitoring are built into Harland Financial Solutions' Internet banking solutions.

That all having been said, it's the combination of technology and process, with well-defined control points, that makes the difference between a safe environment and a credit union at risk. Processes around enforcing strong password protection on devices (PCs, laptops, PDAs, etc.) will force the user (or attacker) to successfully enter their password to use the device. Instituting full disk encryption, VPN quarantine, multi-factor authentication, anti-virus, anti-spam, personal firewall, wireless connectivity, and software installation policies will also assist. Using email content inspection and policy engines to ensure that all email sent to and from your credit union meet corporate data protection standards is also an important part of an enterprise practice. Encrypting any sensitive email sent to and from your credit union and requiring vendors and partners to do the same when communicating with you mitigates the risk associated with NPI breaches.

While all these measures will contribute to your credit union's overall security; education is still the key to an effective risk management program. Educational programs that are tailored to inform the employees of a credit union and its membership are the best. Educating members about security precautions when online or when using check and card products can help reduce or at least prevent an increase in fraudulent activity. Educating staff on areas to be aware of and of changing trends in this area also help. Authentication of employees and limiting access to member data on a "need to know" basis is also an important internal policy precaution. Policies, standards, guidelines, and so on cover a wide range of areas, but the important thing is to develop them in a manner that accounts for future growth and ongoing accountability.

If credit unions take advantage of the technology at hand, keep a vigilant eye on internal controls and processes, and provide employees and members with the education and information they need to be a part of the prevention effort - although no one can change human behavior nor completely eradicate the possibility of fraud and security breaches - a strong recipe to mitigate these risks will have been created.



Peter McKellar
Vice President of
Product Development



Contact Info

www.harlandfinancialsolutions.com

Peter McKellar leads product development for the Credit Union Core business of Harland Financial Solutions. He has over 26 years of software development experience, 23 with HFS. He joined UltraData in 1984 as a Junior Programmer and has since held various positions within the Product Development organization focusing on CU business solutions. HFS supplies software and services to thousands of financial institutions of all sizes, offering its solutions in both an in-house and service bureau environment. The company is a leader in core systems, item processing, enterprise content management, branch automation, customer relationship management, business intelligence, origination and document solutions, risk management, compliance training, financial accounting, open documents, mortgage solutions, EFT, self service solutions and performance advisory services.