CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Online, Mobile, Network & Physical - Securing the Spectrum

Credit Unions should be focused on building a comprehensive, layered security model that addresses the security requirements for each of these channels: online, mobile, network and physical. With a layered security model, the weakness in one control is compensated by the strength of another control. Even more critical is the need for a single administrative console. This allows for centrally-managed and integrated security across all of these channels, which prevents having to solve each independently. This could not only result in the administrative effort to manage multiple, incongruent security silos for each channel, but also an inconsistent experience for end users. Ultimately, the strategy chosen should be derived based on the credit union's risk assessment process, to understand where the greatest amount of exposure exists for its members.

Building and maintaining an layered security model is a continuously evolving effort. The concept of layered security is often described as "defense-in-depth", and relates to building a deep or elastic defense model. It requires not only an investment in technology, but also in the people and processes. Credit unions are no different than other financial institutions, in that, they must evaluate and prioritize their security efforts based on the results of their risk assessment process. Additionally, credit unions should be establishing risk profiles for their various 'types' of members. For example, higher risk members with larger account balances who have entitlements to perform ACH or wire transfer transactions should have additional security controls in place to offer further protection.

The same is true for each channel. Understanding the risks and exposure that each channel presents to the credit union and its members should drive the process of prioritizing competing initiatives. Q2ebanking's platform can be leveraged to query cross-channel data and analytics, which can then be used to make more informed, strategic decisions about your ebanking channels, fraud statistics and member behavior.

Q2ebanking's next-generation, single platform approach to electronic banking enables your credit union to provide the latest ebanking products and services - securely - across online, mobile, tablet or voice. The Q2ebanking platform architecture offers integrated security measures across all delivery channels, regardless of the endpoint or device that your members are using for their banking. The common-platform integration allows updates to any fraud configuration changes across all channels, which may be required as a result of a changing threat landscape threats or the periodic reviews recommended in FFIEC's guidances. The key to successfully maintaining a secure environment is vigilance, ongoing education and taking advantage of the various technology tools available. Q2ebanking provides those tools to its customers.

Jay McLaughlin
Senior Vice President & Chief Security Officer

Jay McLaughlin currently serves as Senior Vice President and Chief Security Officer for Q2ebanking, headquartered in Austin, TX. His responsibilities include delivery and execution of the organization's overall information security strategy and data center operations. Jay has over 13 years of technology and security experience within the financial services industries. McLaughlin is a regular speaker at industry events, such as BAI Payments Connect, InfoSec World, Storage Networking World, InnoTech, Western Independent Banker's Operations Conference, and NYBA's Technology & Risk Management Conference. He has been featured and quoted in various publications including ComputerWorld, CIO Magazine, Credit Union Times, American Banker, ABA Banking Journal, BankInfoSecurity.com, and Texas Banker's Association Magazine. Also, he was recognized by ComputerWorld as a Premier100 IT Leader in 2010 for his contributions and leadership over the course of his career. Jay is a CISSP (Certified Information Systems Security Professional) and holds a bachelor of Science degree in Management Information Systems from the University of Central Florida.

Contact Info

www.q2ebanking.com