

## *Meeting the Challenges of Attacks, Breaches & Compliance*

### Mitigating Attacks and Breaches for Credit Unions

It's no secret that 2014 has been deemed the year of the data breach. With massive breaches at seemingly well-protected financial institutions like J.P. Morgan, and retailers like Target and Home Depot, the battle ground has been set. Companies large and small are heading into 2015 wondering how they can fully defend themselves and their customers against attackers - and that includes credit unions. Budget constraints, manpower and available information technology (IT) resources can often dictate what security products, services, and practices credit unions implement. However, a comprehensive security approach that bolsters defenses—and ensures business and member data remains safe and compliant—is not out of reach.

#### Understanding Protection Needs

First, it's important for every credit union to understand its infrastructure and shortcomings, assess what's important for them from an asset protection and compliance perspective and complete a risk analysis. A Penetration Test provides a means to identify, measure, and prioritize potential threats and risks associated with its external, public systems. For instance, if a credit union conducts a large number of mobile or web-based transactions, assessing protections for denial of service attacks is an important consideration factor. However if you have a basic website, a denial of service attack – in which hackers flood a network with traffic to slow or paralyze it – may cause some member inconvenience, but is unlikely to result in lost revenue.

Second, credit unions should also be sure use their budget wisely when looking for the right security products and services and make sure that they are implementing the right tools. If you need a secure email hosting provider, for example, look for one that also ensures compliance of any communications traveling into or out of your organization and prevents data loss.

Third, it's important to never underestimate your risk factor. You may be a small financial institution but given your assets, you need to operate like a much larger business. The second you underestimate the level of risk your business faces is probably the moment a hacker breaks in and steals sensitive information. Develop a plan to protect your business against known and unknown attackers.

#### Start 2015 with Improved Security:

Here are just a few of the solutions credit unions can implement to improve protection against data breaches:

- \* Penetration Testing: SilverSky Penetration Testing is used to analyze, assess, and test the overall integrity of the external network and critical information technology assets, such as servers and devices, to uncover and identify potential security weaknesses and flaws.
- \* Event Monitoring and Response: SilverSky's Event Monitoring and Response service enables organizations to reduce the costs and complexity of network monitoring and improve their ability to respond to evolving threats.
- \* Email Data Loss Prevention (DLP): SilverSky's Email (DLP) solution delivers enterprise-grade data loss prevention features in a flexible and easy to use cloud service. CIOs and IT managers can guard against motivated malicious insiders and accidental negligence by employees to reduce security threats.

To ensure the highest quality security compliance solutions for credit union customers, SilverSky undergoes periodic examinations by the member agencies of the Federal Financial Institutions Examination Council (FFIEC), as well as annual AICPA SOC 2 Type 2 audits. Visit [SilverSky.com](http://SilverSky.com) to learn about available services and how they can protect and help credit unions boost security efforts.



**Andrew Jaquith**  
SVP and CTO



**Andrew Jaquith** brings 20 years of IT and information security experience to SilverSky, most recently as a senior analyst with Forrester Research. At Forrester, Andrew led team coverage for data, endpoint and mobile security topics. In his time at Forrester, he wrote 20 popular reports on data leak prevention, encryption, endpoint security, mobile security and vendor M&A. Notable recent reports include "Security in the Post-PC Era," "Apple's iPhone and iPad: Secure Enough for Business?" and "The Forrester Wave: Data Leak Prevention Suites." Andrew consulted with and assisted 300 enterprise and vendor customers annually with vendor selection, compliance, strategy and effective practices. Prior to joining Forrester, he was program manager in Yankee Group's enabling technologies enterprise group, with coverage of client security, digital identity, and web application security. Before joining Yankee Group, he co-founded @stake, a security consulting pioneer, which Symantec acquired in 2004. Before @stake, he held project manager and business analyst positions at Cambridge Technology Partners and FedEx.

#### Contact Info

[www.silversky.com](http://www.silversky.com)  
800.234.2175