WHITE PAPER

Balancing Act for Credit Unions

COSTS, THREATS AND ACCESS

For credit unions, security is a never-ending balancing act. Today, the desktop computers and mobile devices of employees serve as both repositories of sensitive business and member data and as access points to applications and corporate networks. Comprehensive security must not only protect information, but also safely enable access to it from any device at any time.

Data protection and secure access require extensive security based on strong authentication. But password-based and PIN authentication can be problematic. Employees forget passwords and PINs and call the help desk for assistance, or they write them down and leave them in unsecured locations. According to Forrester, password reset for large organizations has an annual cost of $1M/year.

Credit unions typically have numerous applications deployed, each of which requires different login credentials and the enforcement of password change policies. This makes the headaches and costs of dealing with forgotten passwords even more onerous.

To improve user authentication, many credit unions seek to strengthen their password policies. They tell employees to use longer and more complex passwords, change them more frequently, or use different passwords for each business application. But instead of strengthening security, such tactics often weaken it. Market data shows that users inevitably:

- Write down passwords
- Re-use passwords
- Share passwords

The High Stakes of Security

When it comes to security, the stakes are high for credit unions of all sizes. Legislation such as the Sarbanes-Oxley Act (SOX) and the Gramm-Leach-Bliley Act (GLBA) compel companies to guard the data and personally identifiable information of consumers. Compliance needs like the National Credit Union Administration (NCUA) audit requirements are pushing organizations like never before to develop comprehensive procedures for credential management. Adding to the burden, the number of data breach notification laws continues to grow. Security lapses result in government fines and penalties, and more costs. Data breaches cost, on average, millions of dollars and can lead to business disruption and reputational damage that can impact the business for years to come.

It's more imperative than ever for credit unions to build an impenetrable security infrastructure with strong authentication. But with this must come fast access to information that enables advisors to deliver prompt, competent member service. Credit unions spend a lot of time and money trying to achieve these dual, sometimes conflicting, objectives.

Some credit unions received an estimated 800 calls per month for password resets, costing $13,600 in help desk calls.

Managing Disparate Security Systems Is Costly

A variety of solutions are often used by credit unions to strengthen authentication, security and compliance. The common practice of patching together numerous security systems creates challenges such as additional expenses and unnecessary complexities for IT staff and users. A comprehensive security strategy that includes different products for Windows® logon, password resets, two-factor authentication for VPN and single sign-on (SSO) for enterprise applications can cost a fortune to purchase and manage. It also often results in redundancies in tasks, cumbersome protocols and excessive time management burdens, all of which create inefficiencies. Moreover, complexity for users translates into slower access to the key information that advisors need to provide strong member service.

Bogging Down in a 'Virtual Headlock'

Many credit unions were grappling with these common issues. The company's authentication protocols were handicapping its member advisors. Like many organizations, they used a password-based authentication system. With more than 25 applications requiring separate logins for access, each with passwords that have different expiration cycles, requests from member advisors for password resets were generating an average of 800 calls per month to the firm's help desk. This was driving up costs and adversely affecting service. Based on Gartner's estimates of $17 per call, that's an estimated $13,600 per month in help desk calls alone. Companies password-based authentication systems were undercutting the ability of their member advisors to quickly and efficiently assist members.

Seeking a Solution to Password Gridlock

To increase the speed and productivity of its member advisors, credit unions explored comprehensive security solutions that were not solely dependent on password authentication. They sought a system that would be flexible, scalable, centrally managed and would require no modifications to its existing applications or infrastructure.

Biometrics and HID Global

Biometrics could speed logon access for its member advisors, heighten security and reduce the cost and time it was losing from password-based authentication.

The advantages of biometrics include:

- Convenient - fingerprints can't be lost or stolen
- User-friendly - easy to use and intuitive for advisors
- Irrefutable - links users to their actions
- Fast - delivers prompt, secure access
- Cost-effective - ends help desk expenses from password recovery
- Proven - well-established technology that sets the standard for innovation and reliability

Preventing just a handful of security incidents can easily add up to millions of dollars in savings per year.

DigitalPersona is a leading centrally-managed suite of security solutions that protects data and controls access to PCs and applications. From biometrics to tokens and cards, DigitalPersona makes strong authentication simple and affordable for PC logon, enterprise application SSO and VPN access. It also supports fast user switching on shared PCs using a common Windows account.

Scalabe, easy to configure and provides authentication across shared workstations which is very beneficial for member advisors and roving workers.

This powerful, flexible solution helps credit unions improve security, achieve compliance, boost user efficiency, reduce help desk calls and lower IT costs. DigitalPersona employs a unique, integrated approach that enables the deployment and management of multiple security applications from one single console. It consists of:

- Management options
- Security applications
- Authentication methods

Once an application is enabled with DigitalPersona's SSO module, IT Managers can replace standard, password-based logons with their preferred authentication policy. When users try to log on to managed applications, they are prompted to authenticate based on the policy chosen by the administrator.

IT Managers can choose from a broad range of policies, ranging from no authentication (i.e., single sign-on) to multi-credential authentication with methods such as biometrics, proximity cards, smart cards and even Bluetooth® phones. DigitalPersona's audit and reporting functionality monitors users' activities by providing evidence of who logged on to a given application, when, and using which authentication methods. DigitalPersona's efficient management of multiple security and authentication applications, combined with a low Total Cost of Ownership, helps organizations increase security and compliance while achieving a high return on investment. The solution delivers savings of up to 54% over comparable systems. Based on industry data, an organization with 1,000 seats may be able to achieve cost savings of $340,000 by using DigitalPersona. These estimates do not take into account any monetary reduction from less vulnerability to a security breach, which could easily add up to millions of dollars.

The Evaluation Plan: Three Ring Proof-of-Concept

The IT team of one credit union established a strategy for testing the HID DigitalPersona solution.

Measuring the impact on each of the following key stakeholders was paramount in its evaluation:

- Members
- Member Advisors
- IT Staff
- IT Environment

Internal champions were identified within the company to pilot the solution. The groups selected were considered the "super" users of applications. They included employees that work only with data (finance, the group suffering the most from the problems associated with password-based authentication), those that work with members (member advisors), and the IT staff that would be responsible for managing the solution.

Why DigitalPersona

The trial of DigitalPersona impressed the credit union. It is a scalable solution, providing authentication across shared workstations which is very beneficial for member advisors and roving workers. It also doesn't require changes to applications and snaps right into Active Directory, so it's familiar to IT staff and really easy to configure.

Once a new security policy is configured with DigitalPersona, it is automatically distributed according to the standard Active Directory replication cycle. The ability to centrally manage the solution from the cloud, and its scalability and flexibility, were other key selling points.

HID Global Solution the Right Fit for Credit Unions

The HID biometrics-based solution is well-matched for the needs of credit unions. It heightens security while simplifying numerous everyday tasks.

Secure Financial Transactions And Payment Data

- Access to computers can be securely controlled.
- Member advisers can safely and quickly log on to applications with SSO

The HID DigitalPersona solution delivers savings of up to 54% over comparable solutions.

- Institutions can secure cash transactions and communications with two-factor authentication using fingerprints, smart cards, digital signature or other methods. Detailed event logs track who did what, when.

Processing Payments In The Back Office
Whenever the back office handles transactions involving member data and funds, the HID solution can add strong authentication to PCs or applications for improved user accountability and security.

Accessing Members' Data At The Local Branch
With DigitalPersona, logging on to any workstation or application is seamless and more secure with strong authentication and single sign-on.

Working Remotely
DigitalPersona protects access to company networks for users with laptops. Employees can securely log on to the network using a VPN with the security of two-factor RADIUS authentication — but without the pain and hassles of using tokens.

Adding A New Employee To The Staff
When new employees are hired, their registered fingerprints or smart card credentials are automatically provisioned throughout the environment, so they can access their accounts, applications or virtual desktops from any computer without re-registering or calling the help desk.

Biometric solutions from HID Global help solved password issues. The solution could relieve the strain on its help desk and improve the speed and productivity of the member advisors.

Best Practices for Deployment

To ensure a smooth deployment companies need to craft a detailed plan. It would install DigitalPersona in its IT and Operations departments and then in Financial Accounting — because this department used so many applications and required the most logons.

Building up internal interest and excitement played a key role in creating a positive environment for employees to embrace the change. To create an optimal environment for the implementation we deployed it for key branch staff first to create evangelists who would discuss the benefits of the solution at all employee meetings and department/branch meetings to keep interest levels high throughout the rollout.

From Password Logjams to Savings and Efficiency

To access second-tier applications, some use biometrics while others still use methods such as PIN and/or passwords. The HID solution essentially eliminated help desk calls related to initial logins to our system because our member advisors no longer have a password to forget, But some employees still use passwords and other means to access the next tier of applications, so the help desk continues to field some calls for password resets.

The HID DigitalPersona solution allows credit unions the following benefits:

- Member advisors gained a net of 1,000 hours of time per year.
- Advisors can better assist members because they no longer waste time on login issues.
- All employees can easily use their fingerprint to get into applications, even ones they don't use often.
- IT is no longer inundated by password reset calls.
- Fewer help desk calls save at least $90,000 in annual IT costs.
- ROI was achieved in months as help desk and compliance costs dropped.
- Preparation for quarterly compliance audits was simplified, and audit requirements were exceeded.
- Fewer user calls enabled two full-time help desk employees to work on other projects.
- New applications are more easily introduced to the company's IT environment.

Unanticipated Benefits Provided an Unexpected Bonus

DigitalPersona allows a company to mandate the use of only biometrics for authentication, or it provides the latitude for a company to indicate when it wants to use biometrics and when additional vehicles for strong authentication can be employed, DigitalPersona is a great, flexible system that financial institutions can use to reduce or eliminate help desk calls, if they so choose.

In addition to deftly and seamlessly handling authentication, DigitalPersona enhances security, strengthens regulatory compliance and also gives member advisors the freedom to easily bounce between systems to access the applications they need, The credit union is so pleased with the results that it is now examining other ways to incorporate biometrics into its business strategy.

Lessons Learned

Credit unions that have incorporated HID DigitalPersona biometrics solution have learned several valuable lessons. These include:

- Provide a solid foundation for success by developing a strong, comprehensive project plan.
- Delineate the details and timing of the roll-out; specify the locations, departments, and people.
- Clearly define how biometrics aligns with each of your current business strategies.
- Determine how to capitalize on the opportunities adopting biometrics will create.
- Identify evangelists within teams, branches, departments and management, and provide them with opportunities to generate excitement and awareness, and educate your staff on biometrics.

Pressure on credit unions to protect the data of members continues unabated. Meanwhile, improving member service, lowering IT costs and giving employees unimpeded access to information and applications remains critical. As the success of Credit Union illustrates, a comprehensive security solution featuring strong, but flexible, authentication options greatly facilitates achieving these objectives.

For credit unions seeking to enable secure access to applications and information, increase productivity, lower compliance costs, and reduce the administrative burdens and rigidity of password-only based authentication, it's time to incorporate biometrics into your business strategy.

2019-11-13-hid-iams-costs-threats-access-wp-en

PLT-04846