

**Data Loss Prevention
And
Internal Data Risk Management**
Are you playing
Russian Roulette?

A Desktop Security White Paper
for
Credit Unions

June 1, 2007

Copyright © 2007 All rights Reserved.

"Helping Credit Unions Work Smarter, Not Harder"

13100 44th Avenue North ● Plymouth, MN ● 55442 ● 763.557.6484
<http://www.intellectualdimensions.com>

Security, the Impossible Dream

The picture to the right is from an old Schlage Lock advertisement and hung behind my father's desk for as long as I can remember. It was not until many years later when my career turned towards executive level information systems management that the picture changed from a funny cartoon to a realistic approach to data security.

My father was instrumental in implementing and enforcing Information Systems Policy for the U.S. Army Field Artillery Software Development organization back in the early 1970s. He once told me that the only truly secure computer system was one that was turned off, unplugged from everything, and locked in a magnetically shielded vault behind a welded shut door. While a "cold and dark policy" like this one significantly reduces vulnerabilities and fosters a very manageable risk model, it does present a certain usability problem and would wreak havoc on your uptime reports...it might also put you out of work.



The trick behind security is to thoroughly assess your vulnerabilities and carefully balance risk with access, availability, connectivity, usability, manageability, and policy. You must carefully and accurately determine where your vulnerabilities exist and this must include a self-maintaining infrastructure that protects, logs, and notifies of real threats; anything less is Russian roulette.

“Those who trust to chance must abide by the results of chance.”

--John Calvin Coolidge
(1872–1933)

30th US president, 1923-9

Unfortunately, this is easier said than done, particularly in the context of budgets, the need for external systems/remote connectivity, and technologies that are becoming more diverse and complex. Risks change by the hour. Tools, skills, policies, and procedures quickly lose their edge if not polished regularly. A security solution must be capable of providing real-time monitoring, and must

be able to adapt to an ever-changing environment. Make no assumptions. Trust no one. Any credit union that has individuals accessing potentially sensitive or confidential data has internal vulnerabilities.

The Threat Within

While many will say that the internet has done more for knowledge management, global communications, and information sharing than any other effort in the 20th Century, it has also

created an enormous series of vulnerabilities that are difficult and expensive to mitigate. According to Gartner analyst Richard Hunter, “more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses”. The primary danger has shifted from external intrusion to internal data leaks by employees. Employees who are permitted access to sensitive data and unknowingly expose that information in emails or maliciously remove data by copying it to an external device are your greatest security risk. However, consider that in many cases access to and utilization of this data is considered part of their job. Many sources of vulnerability involve neither the internet nor remote connectivity; you will find that the greatest security risks are not only at your back door, but are already inside your house.

The most important part of your security infrastructure is a formal Security Plan, supported by a series of documented security-related policies and procedures. For years, credit unions have taken the necessary and extreme perimeter security measures to protect against external threats; hackers, worms, Trojans, spyware, and other malicious intrusions, but until recently there has been little focus on insider threats. Even with your most trusted employee, leaks and removal of confidential member information can and does occur.

Even with your most trusted employee, leaks and removal of confidential member information can occur.

The cost of confidential data loss and theft and its impact on a credit union is immeasurable. At stake are your reputation, your members, and profitability. With internal data leakage, it is not a question of if – it is a question of when and how often.

Take, for example, a situation where a CTO of a credit union inadvertently exposed all of the credit union debit card numbers and member names while e-mailing an unencrypted file to a third party vendor, despite a sophisticated internal security infrastructure. The CTO has network security clearance to transmit and FTP files and knows that files containing secured data must be encrypted; yet, he made a simple mistake by including unencrypted critical information as an email file attachment. We have also observed Member Service representatives capturing screenshots of account summary screens and emailing them to members. It was good member service to quickly provide the information the member needed, but what if it was intercepted while being transmitted via the internet? Think about how many times you have sent an email to someone in error. We have spoken with many marketing departments that routinely send member information to mail houses and other third parties for analysis – in all cases the credit unions had an information security policy in place, but none of these files were encrypted because policies are not automatically enforced and no record of the events exist. How much sensitive information is contained within electronic communication and attachments that are sent to members or third party vendors?

What are the risks

There are many means by which your employees can inadvertently expose sensitive member information; instant messaging, USB storage devices, CDs, portable music devices, phones, and other infrared devices pose the same threat. The devices that make communication faster and easier are the same devices that can be used to breach confidential data. How many times does a staff member insert a USB drive to save a file? Maybe they are going to work on a project at home and are authorized to do so – have you ever lost or misplaced a USB device? Thumb drives, portable

music devices, and other USB devices have been the focus of security risks in recent months, but what about infrared devices? Have you *really* considered where all the logical risks are?

Another channel by which employees communicate information is Instant Messaging. Instant Messaging is a quick way for employees to communicate with fellow employees and friends; however, it can also be used to transmit data to people outside of your network. Another communication method that deserves a great deal of security attention is *outgoing* email. Most credit unions utilize filters limiting attachments by file types or content. For every security measure that is put in place, human nature guarantees that a “workaround” will be discovered. If your email system blocks .doc or .xls file attachments, employees will simply change the file extensions or use their personal web mail to communicate. There are even USB devices that encourage secretive web access by advertising that they will bypass your security and tracking. Additionally, employees that perform work on laptops may compromise data while they are not connected to your network. That “unconnected” PC could contain sensitive information -- how do you enforce your data security policies when a laptop is not connected to the primary domain?

Our presumption of staff honesty and ethics parallels the presumption of innocence by which our judicial system is built. Just as individuals are innocent until proven guilty; each staff member is honest and trustworthy unless they act in a dishonest manner. Unfortunately, the temptation of gain or profit from selling sensitive member data does exist. In this age of technology and convenience, obtaining and moving sensitive information without being noticed has become a relatively non-technical task. Utilizing USB thumb drives and CDs to copy data is commonplace, but there are other channels to consider – infrared or USB ports may be used to transfer files to a portable music device, phone, or even a camera. All of these electronic communication devices can be used to copy sensitive data. We would all like to believe that this would not happen within the credit union industry, but, the sad reality is that it has already occurred. There have been several cases in which employees have maliciously stored sensitive member information on removable media and sold it for profit. Within the past year, one credit union even made the cover of the Wall Street Journal and spent an enormous amount of money to restore member confidence, as well as transfer membership numbers, and reissue debit and credit cards.

Member Service and Security – the Balancing Act



Once the risks have been identified and policies crafted to address them, the next challenge that arises is the unfair balancing act between member service and security. Protecting sensitive or confidential data used during the course of daily business, without compromising member service standards or making it difficult or inconvenient for the members to do business with you, is the balance that must be achieved. Many credit unions address the challenge of internal data security by developing a policy that dictates how sensitive information is used and transferred by employees. The challenge to compliance and enforcement of any policy is the human factor. Employees may be inadequately trained, forget to follow policies, make mistakes, or make inappropriate choices. Most sensitive information that is lost by internal leaks is unintentional. The impact of the loss, however, is not

determined by intent but by financial loss, punitive fines, loss of reputation and diminished member trust.

Internal data threats can use various electronic media sources, but all of the threats have one thing in common – they start at the keyboard. Total lock-down security solutions that protect data may sacrifice employee productivity as well as member satisfaction. The challenge is to enforce PC desktop security without inhibiting staff's ability to perform their jobs in the most efficient manner possible. This challenge becomes more complex as the need for electronic communication methods increases. The use of corporate email, Webmail, and instant messaging as channels for distributing data makes the control of sensitive information leaving an organization a substantial challenge. Moreover, the proliferation of mobile storage devices, such as USBs, CDs, DVDs, portable music devices, and cameras, which allow employees to carry sensitive information outside the organization's boundaries creates an even more complex challenge. In summary, the very tools used to provide service and increase productivity are the vehicles by which data is leaked.

Protecting sensitive or confidential data used during the course of daily business, without compromising member service standards or making it difficult or inconvenient for the members to do business with you, is the balance that must be achieved.

More than Data Loss

The cost of confidential data loss and theft and its impact on a Credit Union is immeasurable. At stake are your reputation, your members, and profitability. The risks of inadvertent or deliberate disclosure of confidential information and intellectual property range from legal exposure to competitive disadvantage. A privacy failure, even a merely perceived failure to protect member data, can result in loss of member trust, affect member retention, and cause significant damage to your brand and credit union reputation.



In today's increasingly information-intensive businesses, technology is an integral part in the protection of sensitive data. A security solution must do more than just monitor perimeter activity; it must protect the data from leaving the desktop at all logical exits. Bulk monitoring such as proxy servers and mail content filter simply are not enough. Tracking real internal threats amid massive amounts of data is impossible without an automated security solution that is actively aware of all activity that takes place on the desktop. What is needed is a real-time view of internal risks based upon the credit union's security policy in order to proactively protect critical data from all identified risks and comply with regulatory mandates.

All discussions about internal data security risks must also include the many regulations and compliance initiatives that impact the management of sensitive information. *Sarbanes-Oxley (SOX)*, *Gramm-Leach-Bliley Act (GLBA)*, *National Credit Union Administration (NCUA)*, *State DFIs*, and *Payment Card Industry (PCI) Data Security Standard* are examples of government or industry regulations or agencies that dictate

The value of compliance is more than achieving a passing grade or escaping a fine; it is protecting your business from financial loss as well as loss of reputation.

how access to sensitive information should be managed. The value of compliance is more than achieving a passing grade or escaping a fine; it is protecting your business from financial loss as well as loss of reputation.

The Solution – Managing Internal Threats Where They Occur

Complete internal data security solutions need to actively control and block the flow of sensitive information and ensure that policies are being proactively enforced. This requires proactively monitoring user activity and preventing security breaches before they occur.

Given the volume of internal data transactions, and the various methods of data communications, prioritizing the real threats without an automated solution is virtually impossible. The right solution is a complete internal data security solution. Complete internal data security solutions need to actively control and block the flow of sensitive information and ensure that policies are being proactively enforced. This requires proactively monitoring user activity and preventing security breaches before they occur. The focus needs to be on automated, real-time enforcement, rather than exhausting resources on the impossible task of trying to manually review data logs, which at best, results in reacting to security incidents well after the fact. Security policies are only successful if they are easy to implement, do

not impact employee performance, are repeatable, and provide an auditable incident resolution workflow that manages security events in real time. In cases where investigation is important, products should include the ability to transparently monitor activity and content so as to not alert the subject(s) of the investigation.

In general, there are two methods for delivering internal security leak solutions; network and agent-based, with advantages and limitations for each. Network based solutions allow for faster deployment since only a small number of devices (depending on an organization's size and need) need to be centrally deployed, and devices are protected as soon as they are connected to the corporate network. This is particularly useful for employees and contractors that may bring in their own computers for work use. While agent based solutions take more time to deploy to end-user clients, they have the ability to monitor all desktop activities. Desktop agents allow for security and coverage of mobile users who take their computers to foreign networks, such as home networks or hotels. Few vendors provide both types of solutions, so consider layering network and agent based solutions from different vendors as a unified solution in order to allow your company the flexibility of deploying the type of solution that most fits your specific needs. Please note that only a few agent-based solutions have the ability to control data access based on content, so ensure that any agent solution examined is capable of meeting your data protection requirements.

There are several important factors for credit unions to consider when evaluating an internal information protection and control solution. The most important tools for securing sensitive information from internal security leaks in complex enterprise environments must include the ability to:

- ✓ Monitor internal activity and identify internal threats at the desktop
- ✓ Centralize easy-to-manage security policies that may be customized by logical groups of users, based upon job function

- ✓ Easily identify suspicious activities and recurring patterns of malicious activity
- ✓ Provide real-time, continuous monitoring of all critical desktop activities
- ✓ Ensure relevant regulatory controls are enforced
- ✓ Monitor all information leakage methods and provide alerts when these activities occur
- ✓ Log all desktop activities and information needed for audits
- ✓ Monitor and enforce security activity without impacting user performance
- ✓ Provide comprehensive reports on security activities, suspicious events, and policy exceptions
- ✓ Provide reports and alerts for tracked security events
- ✓ Support customizable, real-time alerting mechanism for critical activities
- ✓ Easy-to-deploy to workstations and easy to upgrade
- ✓ Provide silent or enforced controls based upon user and activity type

The right automated security solution must include the ease of managing, monitoring and securing internal threats but just as importantly, it must be flexible enough to allow data security to co-exist with your service and performance standards. Sensitive data must be protected through real-time event logging, encryption, blocking, and monitoring at the desktop while still allowing employees to perform their jobs effectively.

Your security solution should not be limited to just “products”. Your solution should include a dedicated team of experts to help assess your internal information security risks and to assist in designing security enforcement policies that are right for *you*; one size does not fit all. Compliance management and the challenge of demonstrating and maintaining IT compliance is not just a checklist with a true-or-false, pass-or-fail technical check. The key to implementing a successful security solution is to understand the business requirements of your organization and to balance them with policies and regulations, credit union operations, member service considerations, and employee education. It is virtually impossible to do this effectively without an automated security event and enforcement tool, analysis expertise, and ongoing monitoring and management.

Information protection and control will be a major security concern for credit unions over the next several years and is likely to receive additional and focused regulatory attention. The repercussions of ignoring internal data security range from loss of reputation, regulatory action, and loss of profitability to legal actions and business dissolution. The topic in and of itself is complex; additionally, when internal data security is implemented so as not to negatively impact member service, employee productivity, or the member experience, it can quickly become even more daunting. Don't play Russian roulette with your sensitive and confidential member data. With the right tools, the right process, and attention to detail you can secure your sensitive data without sacrificing member service or employee productivity. Remember, with regard to internal data leakage, it is not a question of if – it is a question of when and how often.

With the right tools, the right process, and attention to detail you can secure your sensitive data without sacrificing member service.