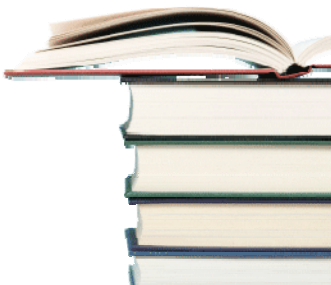




CTH Technologies, Inc.

Protecting Your Credit Union

WHITEPAPER





Protecting Your Credit Union's Financial Enterprise Data from Insider Threats

Today's credit unions face a real risk of insider data loss. This threat can be from disgruntled or ex-employees with malicious intent or honest employees making a careless mistake. These risks can be minimized greatly with the deployment of a comprehensive DLP (Data Loss Prevention) solution that rests on the security fundamentals of identifying vulnerable areas, device control, application, and sound monitoring and reporting practices.

Introduction

In today's financial environment, employees, members, and business partners can easily access more business and financial information than ever before. It's available in real time and usually with a simple click of a mouse or press of a button. But along with the great opportunities this kind of accessibility affords, comes a tremendous amount of risk that must be addressed.

Whether a malicious insider steals information for personal satisfaction or monetary gain, or a valued employee makes a negligent mistake to allow unauthorized account access, the results are the same.

Credit unions stand to not only lose money that's stolen, but there are also legal fees involved, costs to report the breach to members and compliance organizations, and perhaps most important brand damage and member departure. Historically, credit union members have shown loyalty. However, a recent survey by the Ponemon Institute showed that some credit unions reported up to a 20% departure of members once the organization suffered a data breach. In today's economy the financial industry now ranks 4th overall in customer turnover as a result of a breach, ranking just behind the pharmaceutical companies, communications, and healthcare. But what's interesting to note is that the Ponemon Institute also discovered the average cost of a data breach in the financial sector has gone from \$249.00 in 2009 to \$318.00 in 2010 while the average cost across all the other sectors has gone from \$204.00 to \$268.00. That's a \$50.00 difference. Clearly, these risks cannot be ignored.

Tails of the Internal Risks

Be it accidental or otherwise, it's a given that an internal data breach can literally bring your organizations to its knees if proper measures aren't taken. To truly neutralize the risks, IT departments must understand how employees, members, and business partners are engaging with intellectual property and available information.

Almost every organization has solutions like firewalls and anti-virus software in place to protect themselves from some hacker on the other side of the globe. These solutions are obviously much needed but statistics show that some of the biggest security problems credit unions face may originate from fellow employees.

In the past year, 72% of credit union data breaches occurred at the hands of an insider and that figure is on an upward swing as financial organizations around the world continue to suffer from the results of 3 years of economic uncertainty. The fact is that insider data attacks have the potential to cause the biggest losses to your

credit union. Trusted employees can know where high-value information is and how to access it and, in some cases, management does little to track what these individuals are actually doing with the information.

In today's market it's hard to imagine that the majority of financial institutions have done little to combat any of these internal risks. A recent survey of 2000 IT leaders in the financial sector showed that only 26% of all enterprises have measures in place to mitigate insider risks, and only 15% of employers perform an audit of the documents that former employees leave with. Most insiders are successful because their credit union simply does not have the proper tools in place to enforce policies or even monitor employee activity. Credit unions must draft security policies and have in place automated enforcement which the employee adheres to.

Without question, one of the most dangerous and prolific areas of insider threats and data loss is the USB drive and other unchecked endpoints. According to analysts, over 3 billion drives were shipped in 2008. With down-sizing and high rate of layoffs, it's a given that unauthorized data is certainly leaving the credit union. In fact, a recent survey showed that 59% of laid-off employees admitted taking credit union data with them and of those 79% say the employer had policies in place against such practice. Policies have little or no value unless the proper tools are in place to automatically enforce those policies.

Unfortunately, most credit unions today are not taking the appropriate steps to adequately protect themselves from unauthorized data leaving the workplace, either by USB drives, laptops, or mobile devices. Another survey showed that 25% of employers have a policy against taking work home, but 50% allow them to do it anyway. Employers know USB drives, laptops and other mobile devices are unsecure and pose a threat to data loss but are reluctant to impose restrictions. It's not a matter of "not trusting" your employees, it's just that you are counting on them to always make the right decision and do the right thing. Remember, over 70% of internal data breaches are accidental.

Ranking Insider Threats

1. Tellers and Traders
2. Administrative/Back Office Workers
3. Technology Workers
4. Executive/Senior Management
5. Call Center Employees
6. Business Partners/SEG's

Mitigating the Risk Factors

IT departments must eliminate and neutralize the means and opportunities for internal breaches to occur and possible crimes committed. Creating strategic policies and automating the monitoring, enforcement, and reporting of those policies cannot only prevent hackers from accessing information but also give a much better understanding of how employees are engaging with intellectual property to prevent abuse.

Here's a good start to implementing a DLP solution:

Know what's in your environment and where your vulnerabilities lie. An agent based scan, plus assessment of your most critical areas can provide the necessary information to make a well-informed and proper decision.

Have the necessary tools needed to enforce your policies. Policies are only as good as the paper they are written on unless you have the tools to automatically enforce them. It's important to have the ability to set flexible policies that can authorize only certain applications for certain users and not others.

Control and monitor devices. It's imperative to deploy systems and practices that automatically enforce what devices are used by what users on what machines. Also you must be able to track what information is being

moved on these devices. While these devices provide benefits to a more efficient workforce, they also must be monitored because of the large capacity to store information.

Read your reports. In other words, audit yourself. Regular auditing will give insight into the effectiveness of your policies. They will confirm what your users are doing, what data is being moved and where and if some new risk areas need to be addressed.

Conclusion

If you do nothing else, in order to have the most basic internal security solution and meet compliancy regulations, you must address your most vulnerable risk points, or what we call "The Big Three". They are e-mail encryption, end-point protection, and web monitoring and filtering. The CTH Technologies SecureCARE software solution provides you the features to immediately address these risk areas along with a wide range of comprehensive features to address other risk areas or handle future needs as they arise, all integrated under one umbrella and for one small monthly fee.

"There's lots of ways to lose data, some you would never think of that could be very costly.

We're very happy with the CTH Technologies solution."

Ed Berg, CEO First Northern Credit Union

About CTH Technologies, Inc.

CTH Technologies now offers a unified Business Solutions Management platform that secures, simplifies, and automates IT processes. It also improves decision making, provides performance analytics and integrates data workflows across all technology platforms. Security remains the lead focal point within our solution suite offering. Our technology provides Enterprise Information Protection solutions that enable sensitive customer, patient or company data to move securely within large enterprises or small businesses, greatly increasing collaboration, enabling business processes and meeting regulatory compliance requirements for all of our customers.