

CONNECTED



AN ELECTRONIC REPORT FROM THE CUNA TECHNOLOGY COUNCIL

August Summit Promises Education and Fun-In-The-Sun!

Watch your mail and visit the Web site (www.cunatechnology-council.org) for all of the latest important information about the upcoming 6th Annual CUNA Technology Council Summit! The Wyndham Palace Resort & Spa in Lake Buena Vista, Florida will be the host of this year's event; mark your calendar for August 15-18, 2001.

Take advantage of lower airfare rates by booking now. This promises to be one of the best all-around conferences you can attend this year. The educational sessions have never been more timely, or relevant. The location of the summit could not be more fun for you and



your family. You can register online at our Web site. Here are just some of the sessions that will challenge you to rethink and retool your career and your operation.

- * Top Ten Technologies 2001
- * IP Telephony and Convergence
- * Account Aggregation in Credit Unions
- * The Changing Role of Call Centers
- * Security and Privacy Vulnerabilities
- * The Future of ATMs

* Communicating With Non-Technical Staff
These and many more sessions will be featured at CTC's 6th Annual Summit: eMagine-IT! We look forward to seeing you there. ♦

Points to Ponder

Do you refer your colleagues to the CUNA Technology Council because you care about their careers? Or do you refer your colleagues to the CUNA Technology Council because you can win free stuff? Or is pondering pointless?

You're on your toes when you refer new members to the CUNA Technology Council, because you can earn big points. And you can win big prizes because those points add up.

Then you can trade the points for free stuff, like hats, shirts or even a free conference registration!

Ask your colleagues to visit www.cunatechnologycouncil.org and list your name as a referral when they join the technology council. Let them know that they'll be able to brainstorm and network with other credit union professionals who are in their shoes. It's an offer they and you won't want to pass up. ♦

Attention Members: Act Now to Enter the Best Practices Program!

Credit Union technology professionals know that finding the right solution to a problem or situation often is determined by understanding and developing the best approach to accomplish those issues. While there may be no right way or wrong way to face a technology challenge, there is most certainly a BEST way!

Beginning this year, the CUNA Technology Council will offer Best Practices 2001—an opportunity to recognize individuals for the hard work they've done behind the scenes, unnoticed by many, but which contributes significantly to the overall success of a project or their credit union. Technology Council members are invited to submit their Best Practices

entry to this first-ever recognition program. There is no fee to enter the competition for qualifying CTC members.

In 3-5 pages (double-spaced), describe the challenges you faced and the solution(s) you developed to achieve success. Please be as specific as possible and detail particular goals (to accomplish a financial goal; to meet a challenging deadline; or, to develop a procedure for automation and/or efficiency).

Each scenario entered will be judged on the strategy, process, application and results achieved. One first-place recipient will be selected from each of the five categories listed below and presented with an attractive plaque. Winning entries also will be shared with conference attendees during the Technology Summit membership lunch on Thursday, August 16, 2001 in Lake Buena Vista, FL.

Hurry, the entry deadline is June 1, 2001! Please submit a narrative of each entry to Cheryl Sorenson at csorenson@cuna.com before the deadline. We look forward to receiving your entries.

Categories:

- **Delivery Systems:** What has your credit union done to successfully change member behavior to use automated or on-line services rather than costly staff-assisted transactions? Or, what improvements in technology has your credit union made to significantly increase convenience to your members?
- **New Technology Implementation:** What new technology (outsourced or in-house) has been implemented that has resulted in reduced costs and/or added efficiencies? Describe how you figured the return on this technology investment.
- **IT Strategic Planning:** Share why your technique for IT Strategic Planning is successful. Who is involved and what is the process? How does your IT Strategic Plan relate to the organizational Strategic Plan?
- **Web Strategies:** Explain how your credit union has made its web site function more efficiently for its members. What sets your

web site apart? Is it a “full-service” site for your members? How so? What technologies are used to make a member’s visit to your site efficient from a business point of view?

Entry Criteria:

- Entrants must be current members of the CUNA Technology Council.
- Projects must have occurred prior to May 1, 2001.
- Entries must be received no later than June 1, 2001.
- A panel of technology-minded CEOs and IT professionals will judge entries from around the country.
- Entrants must be in attendance at the Sixth Annual CUNA Technology Council Summit, August 15-18, 2001.
- First place recipients in each category will receive recognition and a Best Practices Plaque at the annual Summit.
- If applicable, entrants may submit entries in more than one category. However, the entrant must complete the appropriate entry forms for each category.
- One entry from each category will be selected to receive a Best Practices award; recipients will be selected without regard to credit union asset size and will be notified by June 30, 2001.

Entry Rules

Please limit your entry to 3-5 double-spaced pages. Please indicate the category for which you are entering.

1. Explain in detail a specific (or series of related) project/activity that provided extraordinary results for your credit union. List the specific goals and results of the project/activity.
2. Please list three specific examples of how this practice contributed to the success of your credit union.
3. Provide any additional relevant information to support your entry.
4. There is no entry fee for Best Practices 2001. ♦



To Change or Not To Change Our Host Provider

*Alan L. Darbe
Vice President, Information Services
State Employees Credit Union (Michigan)*

Year 2000 is over, the millennium has started, and the list of things that need to be done continues to grow rapidly. You are concerned that the current host system provider is not able to meet these needs. Now the question becomes, what do I do? The impact of changing a host provider is one of the greatest an organization can have. Very few other changes have the impact to a credit union that a change in the host provider does. Consequently, the reasons suggesting the change, the impact of the change, and what to do if you decide to or not to change should be gathered and analyzed.

The first part of this evaluation is to identify the reasons that are driving the feeling that it is time for a change, and the concerns and the facts behind them.

A common reason for wanting change is a perception that the host provider is not progressive enough. They do not seem to have the products and services or utilize the latest technology needed for the credit union to continue to grow.

Questions to ask here is if there are other ways to provide the services using other vendors? What has your current provider shared about directions and timelines for achieving them and how do you feel about this information?

Another factor, provider pricing (the 'hit me in the gut' feeling that the current provider is grossly overcharging for additional products and services), can lead to a feeling of entrapment and frustration. Often there is no other viable option to many of these items furnished by the provider. What contacts do you have to compare pricing from one provider to another? If others can provide even approximate prices it will let you know what the relative value is and confirm or deny the perceptions.

Perhaps the most important factor is the relationship between the credit union and the provider. A comfortable relationship with the

host provider is critical to maintaining a long-term business partnership. The word partnership is used deliberately to recognize how dependent both parties are on the relationship; one cannot survive without the other. The factors identified above as well as personalities enter into the degree of comfort between them. If you are not comfortable with the relationship, ask what yourself what is the concern and if it can be addressed.

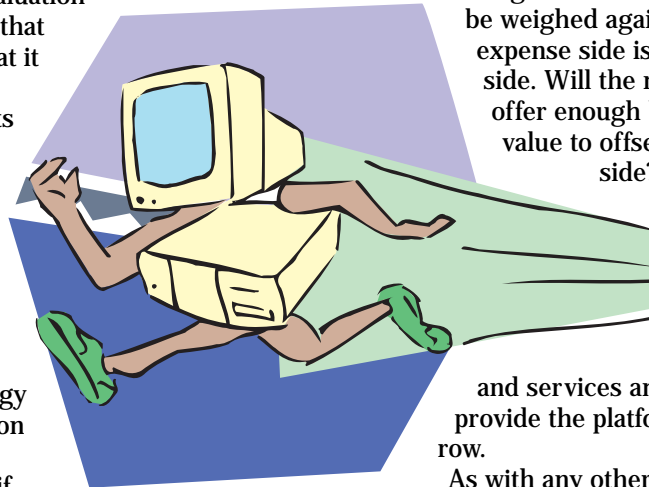
If analysis of all these factors point to the need to change then consider the financial impact of the change on the credit union. Converting to a new host provider is expensive both in money and time. Other than constructing a new branch or other facility, there are few other projects as costly as making a

change to the host system. To be weighed against the expense side is the benefit side. Will the new platform offer enough benefits and value to offset the other side? Some systems do offer a significantly greater range of products and services and will easily provide the platform for tomorrow.

As with any other major capital project, the financial side of the equation should be evaluated. The new provider creates a commitment of several years. The financial expense side of the change includes the actual purchase price of the new system, likely maintenance expense increases both for the hardware and the software, and the loss of income on the investment required.

Another factor involved by the change is the loss of staff time. A new system requires training or retraining the entire organization. Multiplying the number of hours or weeks of training needed times the number of staff will indicate how much time will need to be covered.

Even in areas other than training, implementing a new host provider will involve a significant amount of staff time to review, config-



ure and install the new system. The more powerful a system is, the more choices to be made to implement it. As these options increase, more time is needed to consider the choices and determine the impact on the operations of the credit union.

What other projects or other opportunities will be delayed or missed because of the efforts required for the new system? Can the value of these items be measured and added to the equation?

If, as a result of this analysis, a decision was made to stay with the current provider (at least for a while) what can you do to address some of the issues?

Be willing to make investments in the current platform. Portions of the expenditures that might have been made to undertake a conversion may be allocated to fund development of the products or services using the

provider or potentially another vendor. You may be able to enhance the current host system beyond what you desired from the other systems.

Spend time with the current provider, outline the areas where they are not performing to expectations and inform them of the consequences. Don't threaten them, but inform them of the situation. They don't want to lose you as a customer.

Taking the time to analyze and document these areas will help you validate your decision. The decision to change a host provider is not one to take lightly. When a review of all the factors indicate a change is needed, then a proper allowance for the amount of resources required will make the conversion less painful. If the decision is to stay, then it will be better understood because it is a result of a logical process. ♦

Securing Your Web Site

Darryl Mataya
Vice President
Cyberspace Financial Services (www.cyfi.com)
Madison, Wisconsin

Internet security is like the weather: we love to write and talk about it, but nobody really knows what's going on. That's because we talk about security in the abstract. Those with secure systems that have not been breached or invaded know it, but people rarely talk about it. Those who have been attacked won't talk about it unless they have to, fearing that knowledge of an attack would be bad publicity. These threats are real, they happen to all of us, but there are a large number of remedies that protect you from loss or catastrophe.

Securing your web site can be quite simple, or somewhat complex. It depends on what your site does, where it is hosted, and what mechanisms are in place to protect it. First we need to identify all the threats faced by a

typical financial institution web site. Then we will identify what can be done to protect against those threats.

Threats to web sites fall in the following eight categories:

1. The site is not available. Perhaps the most obvious "threat" to a web site's well being is that it simply must be available.

Sites that are unavailable a high percentage of the time or do not seem to work properly (e.g., have many "broken" links and non-working features) give a visitor the sense that the institution behind the site is not knowledgeable or serious about its operation. From that standpoint unavailable sites simply reflect poorly on the institution's operations and choices.

2. A site gets wiped out. Another obvious issue with web sites is protecting them from being deleted or lost in



some other disaster. In this case, we are basically concerned with being able to restore all of the physical files and resources necessary to make a site operational.

- 3. A site is vandalized.** There have been a number of highly publicized cases where vandals obtain access to a web site and then modify it, often in a non-complimentary fashion! This usually occurs as a result of a web access password being compromised or stolen. In this scenario, it's also fairly easy for the vandal to delete the entire visible site and/or create links to offensive or competitive sites. A big concern in this scenario is the damage such an event can do to the institution's goodwill—something that can be difficult to replace.
- 4. Unauthorized access.** Web sites can hold some member and prospect information or, more importantly, act as a gateway to Internet banking systems, where the threat of damage via unauthorized transactions can be high. This threat refers to the fairly obvious situation in which someone unauthorized to view this information gets access to it.
- 5. Identity theft.** By its nature, Internet activity occurs in a relatively remote setting. Web sites are typically hosted at remote locations not part of the credit union. Our staff can go months without a physical meeting with a web client. The institution can conduct many transactions without ever seeing the member or customer. There are two concerns here. Make sure that customers are always dealing with an authorized employee or representative of the institution. Just as importantly, the institution itself must also concern itself with the veracity of information obtained from its web site. Are the people filling out the loan applications really who they say they are? A relatively complex web site is likely to be made up of multiple components, and different third party firms may deliver those components. In that environment, it's particularly important to be aware of this threat.
- 6. Privacy and protection of customer information.** Because the institution's members and prospects do use the site to send information (say in a loan application), you must ensure that this informa-

tion is secure both when storing it on the web site, and when transmitting it over the Internet to the institution's network or processing system.

- 7. Denial of Service (DOS) attacks.** This is an attack where a web site is bombarded with a high volume of illegitimate requests and is therefore unable to respond or responds slowly to legitimate requests. In this kind of attack, the data and integrity of a web site are never threatened, but confidence in its operation is thwarted when consumers cannot seem to reach the site.
- 8. Password compromise and "clear text".** The largest single exposure you probably face is the loss or compromise of passwords. An unauthorized person gaining access to a web-related password causes most of the bad things that can happen to a web site. Armed with a working password and an Internet connection, they can do quite a bit of damage and/or gain access to many things they should not see. For those reasons, we treat threats to passwords as a completely separate category. In particular, we are always concerned when a password moves across the Internet in "clear text". This refers to the fact that without encryption, email messages, web pages, requests to modify web pages, etc., all move around the Internet in essentially human-readable form. A competent hacker with lots of time and energy can wade through this traffic and discover passwords when they move in this unencrypted fashion.

To protect your web site and its components, your web hosting firm or firms must do much of the work for you. But you have some responsibilities as well. We put the various remedies that are typically used into these two categories.

What Your Host Firms Can Do

- 1. Create on-site and off-site backups for you.** To protect against accidental site deletion, loss, physical disaster, or vandalism, regular and repeated backups of web site information must be made. Many providers do this twice per day; storing one copy on an internal high-speed server and making a second copy to tape and removing it from the facility.
- 2. Monitor the network.** A hosting firm has access to tools that can automate the process of scanning the network for poten-

tial security problems or breaches. In addition to ensuring a network is running, these tools basically look for unusual activity levels and report those for manual follow-up. You should ask your host firms what they specifically monitor (for example, unsuccessful attempts to open up the web site for changes).

3. Use SSL for all remote data access.

SSL refers to the ability for a web site and web browser to communicate using encrypted or scrambled data. Your host firm should be willing and able to use secure certificates and SSL technology for transferring any kind of data between end user and the web site. It is important to note that secure certificates can protect anything: logging on to remote banking, sending a loan application, or logging on for the purpose of changing the site. We strongly discourage any institution from taking application information over its web site without attaching and using a digital certificate.

4. Encrypt passwords. To protect against compromised passwords, a host firm can encrypt all passwords when stored on servers accessible via the Internet or the firm's internal network. In the unlikely event that an intruder gains access to a file of passwords, it would require a significant amount of effort to decode them.

5. Communicate securely with clients.

Make sure your host firm follows guidelines that make it difficult for an imposter to get information about your site. A favorite and very old hacker trick is to phone the network administrator, identify yourself by name as an employee of the credit union, and ask the network administrator to change a password for you.

6. Allow clients to update and modify authorized users.

Your host firm is a potential password leak. While they may be involved in setting up initial passwords, make sure you always have the ability and responsibility to add and remove authorized users and their passwords.

7. Protect the network with a firewall.

A host firm's network is normally going to be protected with a firewall of some sort. It is important to understand, however, that this is mainly for the purpose of protecting internal resources. Public web sites, by their nature, must exist and function primarily "outside" a firewall. A firewall does help protect against vandalism

and potential password compromise by making it very difficult for an external computer to gain file level access to network resources. Note also that this refers to your host firm's firewall and protection. It is perhaps more important that your own network be protected by a firewall.

8. Be able to reproduce your environment.

For disaster planning purposes, your host firm should keep separate physical servers and Internet connections available. Should any of the existing public web servers completely fail, your site can then be re-deployed hopefully in a matter of minutes or hours.

What You Can Do to Protect Your Site

Protect your passwords. Unauthorized transactions or activities associated with a compromised password represent the biggest outside threat to your web site. It is up to you and your employees to safeguard those passwords. The following traditional measures will help greatly:

1. Use a digital certificate to prevent

clear text. A financial institution web site should have a digital certificate attached to it even if the site does not plan to offer on-line applications or other user-entered forms. A digital certificate allows the institution to perform all remote maintenance and data lookup using SSL or encrypted technology. Very simply, this dramatically reduces the possibility that an institution's passwords will ever be viewed across the Internet.

2. Ensure password complexity.

A complex password is difficult to guess. Our own network has experienced what is called a brute-force password attack. In these attacks, automated programs repeatedly try to gain entry using lists of commonly used passwords in the hope that they are able to find one that works. By making passwords a combination of letters and numbers, and by using passwords that are not likely to appear in a dictionary, this threat is reduced substantially. 'ccu3382' is a good password, 'cookies' is not. (A 7-character password made up of 3 letters and 4 digits are sufficiently complex and also fairly easy to remember. Why? Find and read "The Magical Number Seven, Plus or Minus Two", George Miller's famous 1956 study on human information processing.)

3. Rotate passwords.

People write pass-

words down, tell others for convenience and otherwise make it pretty easy for co-workers and maintenance personnel to discover them. Because of this, regular password change and rotation is an essential security policy.

4. Delete unused passwords. With personnel changes, it is imperative to immediately change or update passwords that an ex-employee will already know.

Authenticate people who claim to be working for you. This one is deceptively simple. Have policies in place to ensure your web operators and network personnel are sure they are dealing with the correct people when web activities are taking place. As mentioned earlier, a common method used to steal passwords is to pose as an authorized user.

1. Verify requests. If a network administrator gets a request for username and/or password changes or updates, the administrator should have a procedure to verify that individual if they don't know them

personally or the request is not made in person. Callbacks and supervisor verification are two possible methods.

2. Verify third party individuals.

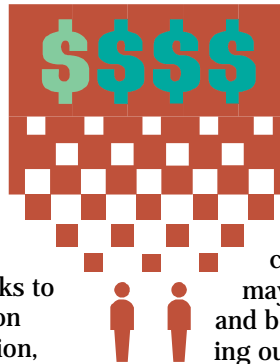
Institutions regularly outsource web development and maintenance work. Make sure your internal administrators or webmasters maintain an authorized list of individuals named to perform web development activities. As with the previous item, separately verify requests for changes to usernames, passwords, or other security-related requests that come from outside parties.

Monitor your content. Your provider is not always in a position to monitor the quality or existence of content in a client's web site. You must make a habit and policy of constantly checking the web site and doing suggested quality assurance checks on the site. This regular activity will reduce the risk of inappropriate activity taking place without your knowledge. ♦

Dan Riley Scholarship Opportunity Available

The CTC is pleased to offer the Dan Riley Memorial Scholarship to qualifying candidates who are interested in attending the CTC Technology Summit. One candidate will receive a complimentary registration to the Summit, plus up to \$1500 in travel and conference-related expenses. The scholarship is made available thanks to support from the Ohio Credit Union League and Universal 1 Credit Union, Dayton, OH. The late Dan Riley was the technology officer at Universal 1.

To be eligible, applicants must meet the following requirements: 1) be a current member of the CTC or be recommended by



a current member; 2) be a full-time employee of the credit union who has the primary responsibility of the IT department; 3) be willing to take an active role in the CTC, such as during the conference; and 4) demonstrate financial need. The requirement of the asset size of the credit union has been dropped. You may find out more about the scholarship, and begin the application process by visiting our web site at www.cunatechnology-council.org. If you know of someone who could benefit from the professional development, mentoring, and knowledge base of the CTC, please direct them to apply. ♦

Don't Forget About Career ExCELL!

If you have been struggling to update job descriptions, post an ad for a new employee, give staff reviews or direct your own career, Career ExCELL is what you are looking for! The Career ExCELL card deck will provide you the tools to perform a variety of tasks including giving you the information to better perform in your own career. Want to move up

the chain or move into a new position? This system will show you which competencies you will need to excel! For more information on Career ExCELL, go to www.cunacouncils.org and click on Career ExCELL in the upper-right-hand corner. ♦

Clark County School Employees Credit Union
**Recycling our Technology Back
into the Community**

Clark County School Employees Credit Union in Vancouver, WA, has been busy giving back to the community through its Information Services Department employees, who have made a special gift of their time and resources to help local schools, charities and community organizations. They have been hard at work refurbishing computers to give to several schools and individuals.

Numerous PC systems were sold to the credit union employees for \$125 per system. All proceeds were given to the Doernbecher Children's Hospital Credit Unions For Kids program. They raised over \$3,000!

Ten PCs and two laptops were donated to the Clark County Amateur Radio Club. This is the second year of donating to this great organization. They are putting the computers to good use.

Many PCs and Macintosh systems, along with various other pieces of equipment, were donated to a program called StRUT (Students Recycling Used Technology). Fort Vancouver High School participates in the StRUT program, which teaches students to refurbish old computers, refurbish servers, and install networks.

The credit union also donated a PC with a modem to Jason Lee Middle School. This sys-

tem will be used for their new automated attendance tracking system, which will call parents of students in multiple languages.

Our Battle Ground branch presented the Information Services Department with a unique situation involving a very special young 31-year-old man with multiple sclerosis. He needed a computer to give him access to many things he could not do. We offered to give him a computer and one of our members, David Richardson, said that he would really like to help us out by updating the computer with a 56K modem, sound card and speakers for a small amount covered by the credit union.

One Saturday afternoon several members of the Battle Ground branch took the computer to Dennis and got it all set up and running. "I wish everyone could have seen the face, the smile and heard the comments of 'cool', 'awesome', and 'I can't believe this!' It totally made my entire weekend and warmed my heart to the max." said Janice Gray, from the Battle Ground branch.

While Clark County School Employees Credit Union donates the computer hardware, the Information Services department also donates its time and expertise to offer these systems to those in need. In addition to these computer donations, employees of Clark County School Employees Credit Union collect donations for the Doernbecher Children's Hospital through the Credit Unions for Kids program on a year-round basis. ♦



© 2001 Credit Union National Association, Inc. All rights reserved.

CUNA Technology Council Connected is a web-based newsletter published four times per year. Send news and CTC information to: Mike Pyltik, manager of technology, Communications Family CU, Saginaw, MI, e-mail: mikep@commfamily.org, phone: 989-249-8221, fax: 989-791-0281. For Council membership and administrative information, contact Cheryl Sorenson, manager - council administration, e-mail: csorenson@cuna.com, phone: 800-356-9655, ext. 4393, fax: 608-231-4061.



CUNA & Affiliates