DCU BULLETIN

Division of Credit Unions

Washington State Department of Financial Institutions

Phone: (360) 902-8701 ***FAX: (360) 704-6901***

January 9, 2004 No. B-04-02

IS&T Best Practices

Trust CC has been performing IS&T examinations under contract for the Division of Credit Unions for the past five months. To provide information to our credit unions regarding Information Systems & Technology (IS & T) security we asked Tom Schauer of Trust CC to summarize his findings in this area for us. This bulletin is intended to assist credit unions to improve IS&T operations by sharing some key best practices.

IS&T Security Best Practices

1. Management/Board Oversight. The most security-minded credit unions regularly involve management and the Board of Directors in all information technology (IT) and information security decisions. They routinely provide reports or schedule quarterly updates concerning risk assessment elements, equipment/software upgrades, or other changes in technology, along with the security ramifications of each. All reports/updates are reflected in the board minutes, along with board approval, disapproval, or actions to be taken.

2. Policies and Procedures. The best information security policies and procedures are those that are board approved; are detailed enough to be usable by IS&T staff, users, and management; and address all elements listed in Appendix A, 12 CFR 748. Policies adopted from other institutions may be a good starting point but they **must be tailored** to the credit union's own unique operating environment.

3. Virus Protection. The best virus protection is that which is always on and is fully automated. Automatic virus program downloads are recommended. Those that are not fully automated should implement a manual maintenance schedule to accomplish the same thing, ensuring that every server, machine, and workstation has been updated and scanned. Staff must be carefully trained to avoid introduction of a virus into the internal network.

4. Risk Assessment. A risk assessment, as outlined in 12 CFR 748, is a systematic analysis of your operating environment in which you identify foreseeable internal and external threats, assess the likelihood and potential damage of these threats, and assess the sufficiency of policies, procedures, and information systems in place to control these threats or risks. A risk assessment is your process to ensure that your credit union has done everything possible to protect your systems—and most importantly, member data—from unauthorized disclosure, misuse, alteration, or destruction. Some of the most effective risk assessments we have seen are simple spreadsheets with separate columns for Threat, Likelihood of Occurrence, Potential Impact, Mitigating Controls, and Conclusion.

5. Patch Management. News stories are frequently aired about security weaknesses or vulnerabilities on various operating systems, such as Windows 2000, XP, Solaris, or UNIX clones. Viruses and worms are successful because they exploit vulnerabilities, which have been identified but that system administrators have simply failed to close with available tools. Closing these vulnerabilities is becoming exceedingly simple, through patch management. Secure credit unions have instituted regular and routine review and installation of released patches. These credit unions have either automated this process or set up a regular maintenance schedule, which includes Windows Updates or similar program updates in other operating systems. Microsoft's patch management guidelines are at www.microsoft.com/security.

Conclusion

Information security is everyone's responsibility, and a strong information security program will help ensure that your member information is protected. In 12 CFR 748 and the FFIEC Information Security Handbook, you will find the tools available to accomplish this. If you review these and implement their guidelines, you will have the confidence that your critical information is secure.

Questions about these changes may be directed to Doug Lacy-Roberts at 360-902-0507 or Mike Delimont at 360-902-8753.