Data Security in a Collaborative Network

Re-engineering our understanding of risk management across multiple networks

Data security is constantly under scrutiny as collaboration and innovation take root among CU*Answers, its partners and clients. In this document, data security policies and procedures across the CU*Answers network are collected and analyzed to assure they are stringent and firmly protecting data of all related entities.

Authored by: Jim Vilker, cuasterisk.com Manager
Revision date: June 3, 2009

This document is an abstract of the full study on data security policies and procedures across the CU*Answers network. To obtain further information, contact Jim Vilker at 800.327.3478, Extension 167.
A New Look at Data Security in a Collaborative Network

Re-engineering our understanding of risk management across multiple networks

Introduction

Data security is under constant scrutiny by CU*Answers, Xtend, our network partners, collaborative client businesses, and our credit union clients. In this day of collaboration, creating innovative ways to provide products and services across multiple credit unions is growing exponentially. This growth has spawned a need to re-evaluate and potentially re-engineer the manner in which we understand data security. In some regards this exercise will not be unlike the one CU*Answers engaged in prior to having the first SAS70 performed. It will yield a body of work in which all data security policies and procedures will be pulled together, analyzed, and ultimately be expanded upon. The net result will be a template of repeatable values across any new collaborative business ventures for us and our clients.

The new template is designed to not only serve as an examination of our security policies and procedures across our network of business units but also to document to warrant the manner in which we address the risks associated these activities. The final result, or goal, is to create a document which a client, partner, or other credit union collaborative business can use to fully understand the methodology used by our teams in managing risks inherent to data security contained in their business models. Although this document will only address those business units in the cuasterisk network, it will serve as a template for future business leaders to use when describing their security processes and policies to their own specific market place. The business divisions that this document will concentrate on are:

Xtend

♦ SRS Accounting
♦ Xtension
  - Conversion support
  - Inbound call overflow
  - CU EasyPay client support
♦ SRS Mortgage Servicing
♦ Member Reach
♦ Audit Link

CU*Answers

♦ Lender*VP Collections
CU*Answers - *Future profiles will be developed for:*

- Client support
- Programming
- Technical, Systems, and WescoNet

**CUSO’s doing business using CU*Base Technical Infrastructure**

- CUbyDesign
- Affinity Management Group
- NMS

This document is expected to yield a pool of business intelligence and a standardized thought process that all business divisions will use. This documented intelligence and thought process will then serve as the basis for a new risk assessment anticipated to be adopted in middle of 2009.

**Standardizing the Outline**

Each operational area will follow the same outline when explaining the security considerations and their inherent risks associated with daily tasks being performed on behalf of our clients. The outlines are developed to serve as a template which can be used consistently across any existing or newly created business division which deals with data access and security. The outline is designed to be intuitive starting with an understanding of what each division does for our clients, followed by all data and systems requirements, continuing with management considerations, and then finalized with monitoring methodologies and considerations.

**What we do**

The outline starts with a description of the tasks which are performed and evidenced by a statement of work, contract, or mutually agreed upon policy and procedure. Understanding and documenting these tasks is critical in determining the scope of data accessibility and will serve as the shoulders on which the remaining steps will be built. A general description of the business unit will be formulated in this section including the division’s reason for being, clientele, and overall data access.
Required data and system access
This second section describes systems and data accesses required by employees who enable them to complete the responsibilities as agreed upon in the Statement of Work. Documentation of these access points produces an understanding of the data elements and increases awareness of identified risks used in the assessment process.

Included in this section is an inventory of:

- Physical systems and the security privileges required to perform these tasks; both internal and external (systems such as Checkfree or corporate central)
- Application data security privileges are required through employee ID and alias settings
- The policies and procedures in place to manage, monitor, or ensure against the risks associated with these given tasks.

The security policies and procedures are attached as exhibits to this document and are referenced in each section.

When defining data access it is necessary to address not only the tasks we perform for our clients but also those items we expressly do not do. An example would be in the client service department where we assist our clients in troubleshooting issues associated with member accounts. In this case we state in our security policy with clients that we will not post transactions or complete file maintenance without their express written permission.

Managing the environment
The next section will describe how we, as an executive team, have decided to manage the risks associated with data access. In some cases the management of these risks is as simple as monitoring daily reports which list the actions of our employees on CU*BASE including all data elements viewed or manipulated. In others a more detailed policy may be required to outline specific security measures including risk mitigating procedures not associated with actual computer access. An example of risk mitigating procedures may include restricting the use of cell phones in operational areas where high turnover is normal.

Technical projects may also be included in this area such as “Privacy 2010”. This project design allows configuration of the system to mask specific data elements and alter the manner in which data is presented on a monitor based on the client’s request. The FACT Act provided guidelines in design of the software. Another area found within this section will include how management has decided to ensure against data security risk. The overall guiding principal of management decisions will revolve around how best to identify, manage, mitigate, ensure, and monitor our business units.
The other major technical project which was released in the spring of 2009 created a new layer of security for the CU*BASE platform. The software allows credit unions to create communities of business partners specific to a single business unit. In doing so it allows our network businesses to limit the access to only those credit unions doing business with that specific business unit. Each credit union then develops its own acceptable security profile for the employees of that business unit. This new security feature has greatly enhanced our ability to manage risk by shrinking the population of accessible client data bases to only those having contractually agreed to do business with that specific unit.

**Monitoring**

The final section will describe how and who monitors the staff activity on the appropriate systems and data bases. This section may also contain future considerations relative to new initiatives such as Xtension. In the majority of cases the owners of the data will be identified as the responsible party and a detailed description of the tools on the system will be reviewed. This could extend beyond systems residing within the CUSO such as debit and credit card processes and other third party vendors external to the CUSO network. The response to data security breaches has been outlined by CU*Answers in previous years and this document will be included in the appendix as a template for our clients to use moving forward.
Audit Link Risk Profile

What we do
The Audit Link division has two interrelated client interactions. The first is an upfront contact consisting of a review of the credit union’s policies and procedures related to regulatory compliance. This contact requires the consultant to review configuration settings and, with the permission of the credit union, update configurations to align with the specific regulation being reviewed and existing policies within the credit union.

The second revolves around the daily monitoring of activity which both members and staff perform on a daily basis. This includes the evaluation of account history and updating tracker records with the intent of keeping a permanent record of the investigation performed. This also includes using analytical tools executed for the entire membership base or for a subset, such as one employee or on high risk accounts, then documenting the discoveries for the credit union to review.

Statement of Work Contained in the Audit Link Contract
The actual periodic tasks performed by Xtend will depend on the rules of engagement workflow defined and documented during the “Original Review Services” process and agreed upon by both Client and Xtend.

Daily Review
As necessary, the following tasks are performed on a daily basis:

- Review BSA reports and verify that the CTRs are filled out correctly and have been filed.
- Review BSA Exempt status list and make recommendations for re-filing the annual exemptions.
- Review Regulation D violation report and contact members.
- Review activity on dormant accounts and verify transactions.
- Review file maintenance logs and verify random selections of activity against physical documents.
- Review wire transfer logs for activity and make recommendations for filing SARs.
- Transaction reversals involving cash or check on member accounts.
- Stale dated check review with recommendations for action.
Weekly Review

As necessary, the following tasks will be performed on a weekly basis:

- Run BSA Report for the prior week and search for evidence of structuring. Make recommendations for filing SAR reports as needed.
- Review wire transfer log and verify that all information is being maintained.
- Review activity on employee accounts and report suspicious activity to Management.
- Run OFAC report and perform investigation on any hits.

Required data and system access

To perform the functions associated with this business unit staff requires access to the following systems and software applications:

CU*Answers internal network

Network access is granted in accordance with the “Data Security Policy” found in Appendix B.

- The privileges are granted to the iSeries by the CIO or CEOs of the specific CUSOs. These employees are not granted high level of access on the production system and do not have file download or data manipulation capability. The category of access for the “Client Service Manager / Representative” will be included in specific risk profiles.

CU*BASE application software

- The access to CU*BASE software containing credit union is limited by the “Community” software and only those credit unions that have contracts with Xtend are displayed on the main menu. The employee ID profile for this division is 89.
- File update functions are allowed if the credit union has granted the appropriate authority. However, this activity is tracked through the applications file maintenance programs.

Managing the environment

To qualify for this position the individual must pass a detailed vetting process including background, reference, and bonding company checks. Employees in this business unit are generally longer term employees with relatively low department turnover. These employees must complete a form detailing all accounts at existing CU*Answers clients and are required to follow the client service policy outlined in the complete risk profile. In that regard management has determined these employees will be given access to the application system in a similar manner as those in the client service department.
Risks which must be managed in this division include theft of large amounts of data and/or manipulation of data through the application itself. Direct downloads are prohibited through the use of the PentaSafe software application which limits access to downloading files from the iSeries. However the risk of member data being compromised by simply completing screen prints from the application itself does exist. This was found to be an acceptable risk as the amount of data which could be stolen is limited and the process itself would appear suspicious to management. These risks have been mitigated through the use of “Community” software which permits these staff members access to only those clients currently under contract with CU*Answers and Xtend.

Another risk associated with this division is the chance that an application configuration would be changed inadvertently during the upfront contact affecting daily monitoring processes. This risk was found to be minute as all configuration changes are completed with the credit union’s management team present. The final risk would be that specific transaction activity by a credit union employee or member would not be caught and be in breach of a regulation or against the law. This was also found to be an acceptable risk in that the probability of this occurring is very low as the credit union is required to review daily work of the teams on a periodic basis. A detailed risk assessment will be completed once a proper format for the document is determined.

Management monetarily insures for the risks stated above through CUMIS for up to $1.5 million dollars per event. Management also ensures for those risks through internal audit procedures and requires clients to monitor all activity performed by employees of Audit Link.

**Monitoring**

Monitoring the activity and associated risks for this department are handled both by internal staff as well as through credit union oversight. Credit unions are required to audit the data system employee report on a periodic basis to determine the activities of the staff. Also, on a daily basis the application system generates a report detailing any employee who completed any data downloads from the application system. Internal staff will monitor and audit the network activity and the application software for data manipulation.

---

This document is an abstract of the full study on data security policies and procedures across the CU*Answers network. To obtain further information, contact Jim Vilker at 800.327.3478, Extension 167.