==========
==========

M A News
Mainframe Audit News
January, 2005
Issue Number 06

==========
==========

Table of Contents

==========
==========

1) Introducing the Mainframe Audit News

This is the sixth edition of the Mainframe Audit News, a vehicle for sharing information about auditing IBM mainframe computers. For more information on this newsletter, including how to subscribe or un-subscribe, please see section 5).

==========
==========

2) Managing Your Audit Planning Through Your View of the Mainframe

The Old View of the Mainframe

Originally we thought of the mainframe data center as a locked room with centralized controls such as environmental controls, disaster recovery planning, and security. When people started moving applications to distributed computers outside the data center, we lost some of the centralized controls, but we gained some freedom and flexibility.

The New View of the Mainframe

For perhaps the last ten years IBM has finally been fully supporting the standards that the rest of the world is actually using. With this change in IBM, people have learned that it is now relatively easy to connect the mainframe to other platforms, such as Local Area Networks, Windows computers, UNIX computers, Novell computers, and even the Internet. We still value the locked-door, centralized controls aspect of the mainframe, but we now also have to view it as just another node on the network. Many would say that it is the most secure, most flexible, most reliable, and most scalable node on the network, but that is not relevant to our task for now.

This new view includes the many tools that IBM has given us to make connections between the mainframe and other nodes easy to implement. These include **MQ Series**, **TCP/IP support for DB2 and for CICS**, and for other middleware, support for **DCE (Distributed Computing Environment)** including the **Kerberos security component** and the **LDAP (Lightweight Directory Access Protocol)** standard for storing and accessing information about users, and full TCP/IP support including **FTP**, **Telnet**, and the **Websphere web server**. (Please note that the Kerberos security protocol may be the only practical defense against sniffer programs on Local Area Networks.) (Many of these acronyms have been explained in earlier issues. We intend to explain the others in excruciating detail in future issues.)

Some people look at these developments, and at how widespread their use is becoming, and conclude that the mainframe is taking over from other platforms. This is not true either. The mainframe is becoming just another node on the network. How much, and what kind of audit attention it needs in your organization is a topic you can address in your audit planning.

How to Apply This New View to Your Audit Planning

Start by looking at the disaster recovery plan, or business resumption plan, for your organization. This is the plan for how to recover critical information processing to support the business in the event of flood, fire, tornado, or similar “disaster”. This plan will have a list of all the applications for all platforms (types of computers). The list will be ranked by how critical each one is to the support of the business operation. As Ronn Bailey of VIP suggests, this will give you a good indication of how critical the mainframe applications are to your organization’s business.

Next, rank the applications informally by the dollar value of the data they process. For the most important applications, determine which can execute successfully on just one platform.

List, or check off, which applications rely on more than one platform to execute successfully. For example, for one application, terminals might be personal computers in a Windows Local Area Network, connected to application programs executing on an AS/400, which relies on a UNIX computer with the Oracle database software to store and to access customer data. All of these platforms would be needed for this application to be successfully recovered.

List or draw an overview of all the platforms (that is, different types of computer) where critical applications execute, showing how the platforms are connected.

Then consider which you prefer, to plan your audits by application, by platform, or by the links connecting platforms.

With these lists, and with this diagram in front of you, you will be ready to start deciding where to allocate IT audit resources in the coming year. Your choice of how much and what type of IT audit resources to use on mainframes will be based on analysis specific to your organization. This is much preferred over audit planning by magazine cover or by the "I know how to audit **x**, so that's what I'll audit this year" school of thought.

3) New Developments and Testing What You Have Learned

New Developments

Two developments in mainframe networking affect the basic set of knowledge a mainframe auditor needs. You remember that the software that controls all networks on mainframes is called **VTAM** (Virtual Telecommunications Access Method). The architecture it uses is called **SNA** (System Network Architecture). SNA has long been contrasted with **TCP/IP** (Transmission Control Protocol / Internet Protocol), which is the standard used by almost every major type of computer, including UNIX, Windows, and Novell.

For a long time, SNA networks relied on **NCP** (Network Control Processors) which are mini-computers dedicated to managing the workload of administering most of the terminals connected to the mainframe. So a terminal might be connected to an NCP, which is in the data center right next to the mainframe. The NCP is controlled by and communicates with, the VTAM software executing on the mainframe.

The **first new development** is wide-spread use of the **OSA** (Open Systems Adaptor) hardware replacing the use of the NCP (Network Control Processor). This allows greater use of TCP/IP, although all telecommunication is still handled by the VTAM software. Some people have suggested that this means the death of SNA networks, but this is not true. Large financial institutions, major corporations, and large government agencies will still need and use SNA networks, even though the SNA protocol is being hidden inside another protocol (called UDP) within the OSA.

This first development requires no special action on your part. However, you should be familiar with the term **OSA** and recognize that the NCP is becoming obsolete.

The **second development** is the recognition of a security risk which is easy to control, but often overlooked in large SNA networks. Imagine that your mainframes are connected by an SNA network named **NetA**. Perhaps you are a bank and you acquire another bank which also has an SNA network, named **NetB**. It is relatively easy to connect these two SNA networks by means of a protocol called **APPN** (Advanced Peer to Peer Networking). This lets a terminal in one of the networks communicate with a program (perhaps a CICS region) in the other network.

For our example, let's say that **NetB** happens to be connected to the network of another bank or of a government agency. We'll call this third network **NetC**. Now a terminal on **NetC** can talk to a program on **NetA**, still using APPN. You might draw a diagram on a cocktail napkin at this point.

The security risk is that a rogue programmer on **NetC** could write a program which would pretend to be one of the real programs on **NetA**. The rogue program would use APPN to pretend to be part of **NetA**. (This is only possible if the APPN security settings are minimized, which is however a common occurrence.) In this way the rogue program could learn userids and passwords or other sensitive information without being detected.

Oh, I forgot to tell you that **NetC** is connected to **NetD**, and that no one in **NetA**'s data center seems to know what country **NetD** is in, or who manages it.

Here are some basic questions to ask to learn whether this situation represents any significant risk in your organization: Ask the VTAM system programmer or the telecommunications staff the names of all your organization's SNA networks. Then ask what other SNA networks they are connected to, what networks they are connected to, and so on until you have a complete map of all the SNA networks that can communicate with your data center. (Don't be surprised if it is difficult to collect this information, and don't criticize the VTAM sysprog if she doesn't know it. In many

organizations it is no one's job to know all this. But if it isn't readily available, you might be concerned enough to pursue the question further.)

Ask the VTAM sysprog what the security settings are for APPN in your data center, and to rate them for you on a scale of 1 to 10 (with 1 being absolutely minimized APPN security). It may take a day or two for her to get back to you, but she will be able to get this information for you fairly easily.

At this point, you can decide whether this risk needs to be addressed more fully in your audit or not. In a future issue, we will try to suggest some further steps if you feel that they are needed.

Testing What You Have Learned

In Issue 03, we described **Job Control Language** or JCL, including the **EXEC card** which describes a program to be executed (usually followed by the DD (data definition) cards describing the datasets to be used by the program). Below is a partial sample of an EXEC card. How many of the following questions can you answer?

//STEP3 EXEC PGM=STUSPGM3, PARM=('JANUARY')

Questions:

1) What program will this cause to execute?
2) What is the name of this EXEC card, that is what step is it?
3) How many EXEC cards might you expect before it as part of the same batch job?
4) Which month's data might the program be processing this execution, and what parameter is passed to the program for this execution?

4) Seminar Information, and the Proverb of the Day

4A) >>>>Seminar Information

This issue we highlight one new seminar for IT auditors, and describe several others for mainframe IT auditors:

- **How to Audit Windows, UNIX, and TCP/IP Security** (June 1-3, 2005 in Washington, DC)

The Henderson Group also offers these "How to Audit..." courses :

- How to Audit **MVS, RACF, ACF2, CICS and DB2 Security** (November 2-4, 2005 in Washington, DC)
- How to Audit **CICS** (April 28, 2005 in Washington, DC)
- How to Audit **RACF** (April 7-8, 2005 in Washington, DC)
- How to Audit **MVS** (April 29, 2005 in Washington, DC

To learn more about them, please go to

http://www.stuhenderson.com/XAUDTTXT.HTM

4B) >>>>This Issue's Proverb of the Day

_____

(Source Unknown) " A Password is like a toothbrush.... it's used daily, must be changed regularly, and you don't share it with others" AND

(from Stu Henderson) “Passwords should be easy to remember, but difficult to guess.”

==========
==========

5) About the Mainframe Audit News; How to Subscribe/Unsubscribe

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily MVS, OS/390, z/OS, and the system software associated with them). This software includes: CICS, DB2, JES, VTAM, MQSeries, TSO, USS (UNIX System Services), TCP/IP, and others. It also includes the Websphere server software which connects a mainframe to the Internet. (Note, we will expand each of these acronyms and explain how the software works over the course of the next several issues.)

The MA News is meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM. We will not make the list of subscribers available to anyone else for any reason.

5A) >>>>To Subscribe, Unsubscribe, or Request Back Issues for the Mainframe Auditors' Newsletter (MA News)

Send an email to: **stu@stuhenderson.com** with the subject field set to: **MA News** and in the body of the email just the phrase you want: **SUBSCRIBE** or **UNSUBSCRIBE** or **BACK ISSUES: 1, 2**

5B) >>>>To Get Questions Answered from the Mainframe Auditors' Newsletter (MA News)

Send an email to: **stu@stuhenderson.com** with the subject field set to: **MA News** and in the body of the email the word: **Question**: (followed by your question, and tell us whether you want your name included or not if we decide to publish your question and answer) Whether we print your question and answer or not, we will try to email you back an answer to your question within five business days. If you need a faster answer, please phone your question to (301) 229-7187, leaving the question on the machine. Please repeat your phone number slowly and clearly.

5C) Tell Us What You Think

We'd love to hear from you, in particular on these topics:

- What do you like/not like about the MANEWS?
- What websites do you know that you want to share with other auditors?
- What topics and/or columns would you like to see in future issues?
- Is your mainframe connected to the Internet and do you plan to audit the security implications of this connection?

Please email your comments to stu@stuhenderson.com. Thanks.
==========