What's Missing in Mainframe InfoSec:
(What We Don't Know We Don't Know)"

Stu Henderson
5702 Newington Road
Bethesda, MD 20816

stu@stuhenderson.com
www.stuhenderson.com
(301) 229-7187

ABSTRACT

In this webcast, an experienced system programmer and security consultant explores possible reasons for the number of security exposures found in our data centers. Even though smart people work hard to secure our system well, hackers, auditors, and reviewers continue to find exposures. Something is not working for us. Now that criminal hackers are pursuing mainframes, we need to make sure we're securing them effectively. While the z/OS system is the most securable platform around, it's not the most secure unless we use the tools we have effectively. This presentation will show you uncommon sources of security weakness and uncommon steps you can take to improve your information security.

Agenda

1. Introduction
2. The Technology
3. The Organization
4. Recommendations
5. Summary / Call to Action

1. Introduction

- We spend a lot of time and money and effort on IT security.
- From the headlines and the audit reports, we know it’s not working.
- If what we’re doing isn’t working, we need to try something else

1. Introduction

- Is it that we don't understand the risks?
- Or that our tools aren't adequate?
- Or we don't know how to use the tools?
- Or we don't know what it is we don't know?

1. Introduction

- We’re going to look at what’s behind some commonly encountered security exposures.
- We’ll address the unknowns
- We’ll recommend how to fix the situation
- The answers in the end will be already familiar, basic management controls

2. The Technology

□ Some of us remember when there was at least one dedicated, experienced sysprog for each system software.

□ Imagine a CICS sysprog with 20 years experience. And a VTAM sysprog, with 25, who retires.

□ And management asks the CICS sysprog to “take over VTAM”

2. The Technology

How many of these long-time technology issues are you familiar with:

□ Residual data on disk and on tape

□ The 17 character dsname security risk

□ DB2 with DDF

□ I/O appendages, User SVCs, APF

□ Change control over system datasets

□ Applids (programs) that use hard-coded lists of userids and paswords instead of calling the security software

2. The Technology

How many of these recently developed technologies are you familiar with:

- UNIX, TCP/IP, Policy Agent, http
- MQ security
- Encryption, symmetric and asymmetric
- JAVA, Websphere, WAS
- Tivoli
- HCD, IODF, Shared DASD, sysplexes
- CICS with JAVA and TCP/IP
- APPN cross network security

2. The Technology

- Experienced tech staff is thinner, with less depth.

- The technology has exploded

- Some common stories

2. The Technology

Some common stories:

(commonly encountered, real life)

- □ Passwords sent over Internet without encryption. Decision was made because some other company's computer doesn't support encryption.
- □ System programming manager not aware of privileged programs added to the system

2. The Technology

Some common stories:

- Management is surprised to learn of an unprotected authorization SVC added to the system years ago

- MVS system programmers surprised to learn of DB2 and CICS sysprogs updating their own APF datasets

2. The Technology

Some common stories:

- DB2 option set so users don’t have to prove their identity over the network.
- Management surprised to learn that SNA network is connected to other companies’ nets without risk assessment. Only one person knows the names of the other companies. No one knows what companies their networks are connected to.

2. The Technology

Some common stories:

- Auditors ask for "baseline document" specifying how options are supposed to be set. No one has one for DB2, VTAM, MVS, SMF, CICS, TCP/IP, FTP, TN3270, Policy Agent, security software, nor httpd

- New Rational development workstation used by new JAVA programmers. Rest of mainframe staff not familiar.

2. The Technology

These common stories involve situations where technology can introduce risk without key people knowing about it. Information doesn't flow where it needs to go.

The result is significant risk that isn't known.

2. The Technology

To Recap:

- Experienced tech staff is thinner, with less depth.
- The technology has exploded; staff and training budgets shrunk
- Common stories

3. The Organization

For effective protection, we need to understand:

- □ Technical risks, translated to
- □ Business, operational risks, compared to
- □ Cost to reduce risks

This requires better information flow.

3. The Organization

For effective protection, we need to understand:

□ What risk assessment is conducted, if any?

□ Who does it?

□ With what knowledge and authority?

3. The Organization

Security administrator is often very good with security software (RACF, ACF2, TopSecret)

But often lacks knowledge of:

- Regulations like SOX, PII, PCI
- System performance and tuning
- Network security, TCP/IP and SNA
- All the tech details described above

3. The Organization

Some common stories:

(commonly encountered, real life)

- Security administrator decides not to use feature (**EOS** in RACF or **AUTOERAS**E in ACF2, TSS) which would protect residual data on disk. Compliance department, Legal department, application owners not aware of issue. Sysprog believes that the feature causes performance problems.

3. The Organization

Some common stories:

- Security administrator decides not to activate various important resource classes (such as **JESSPOOL, VTAMAPPL, DASDVOL, OPERCMDS, UNIXPRIV, SERVAUTH**) or not to define rules because administrator doesn’t understand what they are for, nor how rules should be defined

3. The Organization

Some common stories:

- Security admin discovers digital certificates are expiring, and the only person who understands them retired five years ago

- No one is able to explain in clear detail how the mainframe is protected from the Internet

3. The Organization

Some common stories:

- Several users can update sensitive system datasets, but it's all logged and reported. Volume of updates makes it difficult to review effectively.

3. The Organization

Some common stories:

- Mainframe connected to the Internet for Ecommerce, including FTP, TN3270, telnet, and http (software that talks to Internet Explorer).
- Security administrator not informed nor consulted.
- PAGENT (free, great, mainframe firewall) not implemented.

3. The Organization

Some common stories:

- Auditor recommends that security administrator “review the violations report each day”. Number of violations increases very gradually week by week. Security administrator gets new eyeglasses.

3. The Organization

Some common stories:

- Two data centers combined with different security software. All DASD is shared across all lpars. Both security administrators unaware of implications.

3. The Organization

- Who makes the security decisions, if anyone?
- Who has the knowledge to make them?
- Who has the authority to make them?
- Who isn’t aware of them?
- Is the risk truly understood?

4. Recommendations

Clarify responsibility for:

- □ Identifying technical risks
- □ Identifying regulatory risks
- □ Identifying business risks
- □ Deciding what tools to implement and how
- □ Reviewing all risk and protection

4. Recommendations

- Implement sufficient change control over every system dataset so that no change is possible without manager approving, being aware and reviewing, able to roll back.
- (What system programming manager would want anything else on his watch?)

4. Recommendations

Map what you have and assess the risks:

- □ Lpars, sysplexes, shared DASD
- □ TCP/IP networks, including firewalls between mainframe and the Internet
- □ SNA networks, including adjacent networks and their adjacent networks (You have SNA if you use Enterprise Extender)

4. Recommendations

To know what you've got

- Develop and maintain hardware and software inventory with baseline documents for each piece of software.
- (You need to review all the software anyhow when you go to a new release of z/OS)
- Maintain list of known risks and status

5. Summary: Call to Action

- We all know examples of IT security issues that don’t get addressed, even though good people are in charge

- To fix this, we need to change the way the organization assesses risk, including responsibility, authority, budget, information flow, and procedures

- This won’t come overnight, but we can start it now.

5. Summary: Call to Action

- These recommendations are all basic management controls for any mainframe data center.
- They let you stay in control of the assets you're responsible for
- They clarify where IT needs input and information for the rest of the organization.

5. Summary: Call to Action

- These recommendations protect your security administrator from unwarranted blame.
- They protect the CIO and the sysprog manager from same.
- They can reduce audit costs
- They can help to groom new staff.

5. Summary: Call to Action

- □ You can make your organization’s security more reliable.

- □ If not you, then who?

For More Information

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes:

https://web.nvd.nist.gov/view/ncp/repository

- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53):

http://csrc.nist.gov/publications/PubsSPs.html#800-53

For More Information

- □ Tools to map hardware and to provide system software change control:

www.newera.com

- □ Tools to evaluate cross-network security with APPN and/or Enterprise Extender:

www.net-q.com

For More Information

- Cheryl Watson's Tuning newsletter documents some amazing improvements in Erase On Scratch (AUTOERASE) performance with z/OS 2.1, especially with one particular APAR. She strongly recommends re-visiting whether you use EOS or not, given these improvements. She gives an amazing amount of hard, detailed measurements, backed with clear, detailed technical explanations. More on next slide.

- To subscribe or to see a sample issue,

http://www.watsonwalker.com/sampleissues.html

For More Information

- **Frank Kyne performed erase-on-scratch testing that is documented in Cheryl Watson's "TUNING Letter - 2015 No. 1":**
  - Allocated data sets of 1, 100, 255, 25600, and 63000 tracks
  - Ran a separate job to delete each data set, varying erase-on-scratch on and off, on z/OS V1R13 and z/OS V2R1
- **Frank's results:**
  - Small reduction in elapsed time and EXCP counts for the smaller data set sizes (1, 100, 255)
  - Large reduction in elapsed time and EXCP counts for the larger data sets
    - For the 63,000 track data set, EXCPs dropped from 63,007 to 263
    - Elapsed times decrease between 1/3 and 2/3
- **Once you are on z/OS V2R1, perhaps it's time to revisit erase-on-scratch!**

For More Information

- □ z/OS Manuals from IBM:

(www.ibm.com/servers/eserver/zseries/zos/bkserv/)

- □ Handouts from previous meetings of the NYRUG:

(www.nyrug.stuhenderson.com/handouts.HTM)

Thanks for Your Kind Attention.

Questions to Stu Henderson

(301) 229-7187

stu@stuhenderson.com

www.stuhenderson.com