JUST FOR CIOS

MANAGING MAINFRAME INFOSEC MORE EFFECTIVELY

Stu Henderson
5702 Newington Road
Bethesda, MD 20816

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

ABSTRACT

When a CIO wants to know how good his organization's information security is, it's hard to get a clear answer. When audit findings seem to put your organization in a bad light, it's hard to know how to react to them. Sometimes it's even hard to know how what they mean. It's hard to know how much time and effort to invest in InfoSec and where to invest it.

In this session an experienced system programmer, auditor, and consultant describes practical steps you can take to understand and to manage your organization's InfoSec. You will learn specific questions to ask and how to respond to the answers. You'll learn how to respond to auditors, and how to manage them from the beginning of the audit. You'll learn what your staff needs to do so that you can demonstrate that your InfoSec is as reasonably effective as it can be.

AGENDA

I. Introduction and Constraints

II. Practical Steps
(Four Recommendations)

III. Summary and Call To Action

MANAGE INFOSEC EFFECTIVELY

I. Introduction and Constraints

We all want to know and be able to demonstrate that:

- Our Information Security is reasonably reliable
- At reasonable cost

MANAGE INFOSEC EFFECTIVELY

I. Introduction and Constraints

But a large number of constraints make this difficult:

- Budget, staff shortfalls
- Breadth of techno-babble, social media

MANAGE INFOSEC EFFECTIVELY

I. Introduction and Constraints

Variety of technology:

- MVS, JES, VTAM,
- CICS, MQ, DB2
- USS, the Internet
- TCPIP, FTP, httpd, Policy Agent

MANAGE INFOSEC EFFECTIVELY

I. Introduction and Constraints

Variety of technology:

- Virtualization, hardware and software
- Government regulations, PCI
- The cloud
- Digital Certificates

MANAGE INFOSEC EFFECTIVELY

I. Introduction and Constraints

So what steps can you take to:

- Get your staff to implement sufficient security without hurting other initiatives
- Know where you stand
- Be prepared for InfoSec Audits
- Have answers for other executives

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You think the CEO might be about to ask you if your Information Security is sufficient …

- So you ask your System Programming Manager who tells you ***"It's OK"***

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You think the CEO might be about to ask you if your Information Security is sufficient …

- So you ask your Auditor who tells you "***We Evaluated Your Controls Using Our Proprietary Methodology and We Found Only Minor Weaknesses***"

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You think the CEO might be about to ask you if your Information Security is sufficient …

- So you ask your Security Administrator or Data Security Officer or Chief Information Security Officer, who tells you "***We've Almost Completed the RBAC Project and I've Been Busy Responding to the Auditors' Comments***"

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

So maybe you want to

- Ask more specific questions, and
- Ask people to get you answers if they don't already have them

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

The characteristics of good questions are:

- Have YES/NO answers
- Add up to "How Good Is InfoSec?"
- Break down into manageable pieces
- You can ask other people to verify

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Here's an example of six great questions to ask

1. Can people access the system without approval?
2. Can people access data without approval?
3. Can people access resources without approval?

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Here's an example of six great questions to ask

4. Can people change the rules without approval?
5. Do the right people do three basic functions? (next slide)
6. Is the system software secure?

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Who should do each of these three basic functions:

1. **Approve** access
2. **Grant** access
3. **Review** access

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

The characteristics of good questions are:

- Have YES/NO answers
- Add up to "How Good Is InfoSec?"
- Break down into manageable pieces
- You can ask other people to verify

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You can break questions like: *"Can People Access the System…?"* into manageable pieces

You can ask your staff to break the questions down

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You guide how your staff spends their time by the questions you ask

Ask the right questions

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

The characteristics of good questions are:

- Have YES/NO answers
- Add up to "How Good Is InfoSec?"
- Break down into manageable pieces
- You can ask other people to verify

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Recommendations:

1. Ask the Right Questions

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Say you want to get an answer to data access

- How does anyone tell you that data access is what it should be?

- They need a definition of what data access should be

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

How does that get decided in your shop?

- Anyone gets access just by asking for it?
- The Security Administrator decides which requests to approve?
- Someone separate from Security Admin approves request?

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Your Security Administrator doesn't have the knowledge, nor the authority, to decide who should be allowed to access what data

- You can clarify who does have this responsibility in your Security Policy

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Who has the knowledge, the authority, the ability to:

1. **Approve** access
2. **Grant** access
3. **Review** access

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Use your policy to align responsibility with:

- Authority
- Knowledge
- Ability

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Don't develop the policy yourself:

Develop it with your peers

Ask your staff to coordinate the process

Make sure the policy sorts out who is responsible

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Recommendations:

1. Ask the Right Questions
2. Sort Out Who Is Responsible

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Whoever you request to answer your questions will have one immediate issue:

- To evaluate your InfoSec what do they compare it to?
- Some sort of standard or yardstick

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

You want to manage the yardstick yourself

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Here's how you manage the yardstick:

- Whether you use the six questions suggested, or another set of questions, note the phrase:

  "Without Approval"

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Once you've sorted out who is responsible for approving what:

- Have that person document the approval or **baseline**

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Baseline Documents:

- Specify how options and procedures are to be set up in your shop
- Without them the risk of losing key staff is greater
- To groom new staff have them develop the baselines

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Baseline Documents:

- Auditors ask for them now
- Auditors use them as standards against which to evaluate you
- So manage the standards

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Recommendations:

1. Ask the Right Questions
2. Sort Out Who Is Responsible
3. Have Your Staff Develop Baselines

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Starting with the right questions, you can:

- Align responsibility in your policy
- Have the responsible approvers document baselines
- But what about your auditors

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Manage Your Auditors:

- Use the Scope Statement
- Findings must show relevant, meaningful risk or breaking of a law or policy
- Suggest that they use your baselines as a meaningful standard
- Ask them to answer the big questions for you

MANAGE INFOSEC EFFECTIVELY

II. Practical Steps

Recommendations:

1. Ask the Right Questions
2. Sort Out Who Is Responsible
3. Have Your Staff Develop Baselines
4. Manage Your Auditors

MANAGE INFOSEC EFFECTIVELY

III. Summary and Call To Action

These four recommendations fit together to help you answer "How good is our computer security?"

1. Ask the Right Questions
2. Sort Out Who Is Responsible
3. Have Your Staff Develop Baselines
4. Manage Your Auditors

MANAGE INFOSEC EFFECTIVELY

For More Information:

- The Henderson Group website for newsletters, articles, and white papers (http://www.stuhenderson.com/Articles-Archive.html)
- The Federal government STIGS (Security Technical Information Guides) for various platforms (http://web.nvd.nist.gov/view/ncp/repository)
- Document 800-53 (http://web.nvd.nist.gov/view/800-53/home)