

THE NEW CSO “PRIORITIES” HIT LIST

Version: 1.0 – 27/03/2001 - Clément Dupuis (cdupuis@cccure.org)

Version 1.1 – 28/03/2001 – Added Legal/Compliance section

This document is a compilation of the answers to a question that was posted on the CISSP mailing list about what would be the first three items a CSO should do upon walking into a new environment.

This document is a living document, as such it will evolve with time and feedback is most welcome. I will attempt to keep it updated anytime more messages are posted on the topic. You can send any input to cdupuis@cccure.org.

The latest version of this document will be available from the CISSP Group file area or from the CISSP Open Study Guides web site located at <http://www.cccure.org> under the download menu you will find a category called JOB TASKS.

The exact question posted by Mike (mtonick@aol.com) was:
[In your opinion, what would be the first three items on a "To-Do" list for a new CSO walking into a new environment?](#)

Here are all the answers with very slight editing for clarity. The answers are presented in no specific order of priority. I do believe that they are all points to ponder and worth taking a look at. If you are employed as a new CSO this list can be a very good checklist of items to look at and see where you stand. As mentioned it would even be better to look at this list prior to signing for a new employment as a CSO.

I must also mention that there is no magic recipe and whatever approach you will choose will depend on the situation you experience on the ground. Please read carefully the SOCIAL/CULTURE section below. It will probably be one of your biggest challenges.

THE CONTEXT

Before you get into the list of priorities, I would like to mention a few points that will put the answers in context.

The items listed below are for someone that has just been hired, he has not been promoted from within the company, and he is walking into his new work environment.

Also to clarify a bit further, when talking about CSO we relate to a senior position reporting as a peer to the CIO (not reporting *to* the CIO).

MANAGEMENT COMMITMENT

It is obvious that having management commitment seems to be the #1 priority. It should be something that you looked at even before accepting a job as CSO. Without strong commitment from the highest level you may have lots of difficulties in achieving any of your goals. Here are the answers received:

- Ensure top management is strongly committed to security.
- Get executive level notification of support to all the company concerning "Enterprise" security. This is essential as you are going to have a number of conflicts that this can smooth out before they start. If your CEO is not on board with security, no one else will be. Everyone needs to know that.
- Nail down senior management support (and I do mean SENIOR- the board of directors, CEO, or some other very high ranking group of people) for the role, and outline it on paper including expectations, roles, responsibilities, etc.
- Get top management support and be sure your role, responsibilities and the scope of your job are well defined. As Scott Sanchez has noted also be sure you have that management's support for it as well.

LEGAL/COMPLIANCE

Another aspect to look at is the regulations that you must comply to. Here are some of the suggestions received on the subject.

- What are all the governing regulations? Make a list. Get copies.
- Map the security relevant activities with the project goals and start determining how you are going to manage compliance.

ACCOUNTABILITY

Quickly find out what your relation will be in regards to audits. What does the organization expect from you and your level or responsibilities.

- Find out what the tolerance level is by the Audit Committee of Board for insecurities.
- Find out what the organization believes the accountabilities are for Security (they can vary widely).
- Project implies goals; what is the mission? It should be written down somewhere; if it isn't, look for another job. (Well if you don't know where you're going, then anywhere is good ... but that is contrary to being a CISSP)

POLICIES/PLAN

Another area mentioned by quite a few of the respondents was policies. Here you must ensure that you have policies, review them, update them, create them, see how they meet business objectives etc...

- Review and change/draft policies that establish security in the organization.
- Prepare an Information Security Operational Plan that you can present to the management that lays out your plan of attack. Based on the business, the gaps and the needs you can prioritize the places that you need to request budget, people resources, hardware, software etc.. You need to realize you won't be able to do it all in one year even if you had an unlimited budget (even though it might be fun to try). It is just not realistic to do it all and do it right.
- Get adequate BUDGET & resources (i.e. staff, etc.) for your new role.
- Prepare an 18 months or more roadmap, get senior management to agree to it.
- Annually recreate your operational plan with new goals, a status of the prior year and use it to show management your progress or new needs and why.
- Find out if there's an INFOSEC policy in place - if so, make sure it's current, and if not, get one put together.

BUSINESS OBJECTIVES

The two submissions below clearly identify what your approach should be towards meeting the business objective. The bottom line is always that you must be profitable and your customers must be happy.

- Take a scrupulous look at the company's security plan and how it relates to (or support) the company overall business goals. Understanding this relationship will enable you to adopt strategies and make recommendations that will promote the business and enjoy the support of top management.
- Understand the *business* as best you can. Ok, so you're the Chief *Security* Officer. Big deal. Your company is not in business to "be secure", per se, it's in business to serve your customers and make a profit doing so. It's essential that the actions you take as CSO are consistent with running your particular business in a rational way.

ANALYSIS/INVENTORY

Another huge task consist of taking a quick snapshot of where you stand security wise. Go around, meet people, let them know that there is a new kid in town that they can talk to without fear or reprisals.

- Perform an analysis of business process; current security to establish a baseline for where the company is at with security and prioritize where you feel it needs to go. This is the "where you need to be". Use a "GAP Analysis" to establish the

holes between the baseline (where you are) and the "where you need to be". This will all feed into your strategy.

- Ensure you take a road show, if you have various locations, or just travel around the campus/building and introduce yourself. **YOU WANT PEOPLE TO BE ABLE TO COME TO YOU IF THERE ARE ISSUES SO BE PERSONABLE.** True security officers should never be the ogres they are portrayed as.
- Begin the slow process of assessment - per site - per business unit. Begin coordinating all efforts and focusing the **PEOPLE**. Say you have 1000 employees, consider how secure your information is, how much you can support privacy and protect patient and member rights if you have 1000 security officers instead of 1.
- In conjunction with the policies - draft an overall organizational security plan. Better base it on about a 24 months window to support those portions of the HIPAA Privacy rule that security needs to implement. Remember, you can have security without privacy, but you cannot have privacy without security.
- Take stock of resources available to you (the CSO); the budget, staff and security controls already in place. This is necessary for the CSO's strategies and effective operation.

LOOK AT THE PAST

If your position is not a new position, you can take a look at what has been done in the past. Look at audit reports or any other documents that may indicate if there is any outstanding problems (hot potato) that should be addressed right away.

- Find out if there are audit issues outstanding (see past audit reports).

IMPLICATE

For a security plan or security policies to be effective you must gather people from the different group in your company. Make them feel that it is their plan, make them collaborate and provide input. Once the final version comes out they will feel a lot better about something that they developed instead of something being enforced on them.

- In parallel and in conjunction with the item above - as immediately as possible put together a group from the cross section that can review and approve that policy.

CULTURE/SOCIAL/PEOPLE

This section as I have mentioned above is definitively your biggest challenge. If you deal with 100 people then you have to develop 100 different approaches. Soft skills are as

important as technical skills in helping you achieve your objective and in getting the support that you need in your new job.

- Oh, by the way, institute security company wide in an Enterprise fashion involving HR, Facilities, Finance, Clinical and what ever other departments you have without ruffling feathers! You'll never do it so be ready for resistance - the way to be ready is to ensure the President and CEO are behind you. The only way to be sure of that is to meet them one on one and talk to them and get their note out to the populace.
- Understanding the corporate culture; top management, your peers, and all other system users. What practices and attitudes they are likely to accept or reject. You must be very lucky to get anything done if you do not really understand the corporate culture.
- Get to know the people first. Not just *your* staff (which is important, of course), but the people outside of the security organization from whom you'll need support to be effective no matter what you do. Make friends. Learn to play golf, if you must. Too many IS people think they don't have to be congenial; they just have to be Right(tm). They're crackpots.
- Your company has not only a business, but also a culture. A way of doing things. It's a reflection of many influences, not all of which are positive but equally important not all of which are negative. Sometimes we do stuff blindly because "that's the way we've always done it" but other times there really is a good reason that is not obvious to the newcomer. As Stephen Covey says, "Seek first to understand, then to be understood."
- Figure out what the organization's "security culture" is, and if it is lax or non-existent, start planning awareness training. If it's strong, keep the awareness current.
- Make sure the people maintaining and managing the IT infrastructure (both hands-on people and executives) know what they're doing from a security perspective. If they don't, get them trained. If they do, reward them heavily.

CREDITS

MAINLY EXTRACTED FROM MESSAGES SUBMITTED BY (in alphabetical order):

Bill Campbell	billc@eaglesreach.com
Jack Holleran	Holleran@severnapark.com
Ken M. Shaurette	ken.shaurette@goliath.com
Laurie McQuillan	LMcQuillan@netdes.com
Micki Krause	micki.krause@phs.com
Scott C. Sanchez	scott@gungadin.com

Sefadzi
Tim Senter

sbedzra@aol.com
trsenter@magellanhealth.com