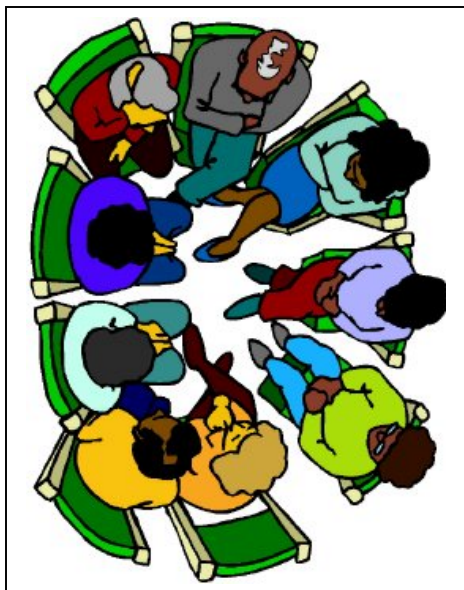


Starting a CASPR Group: Suggestions for Prospective Team Leaders

If you have an area of expertise that you'd like to see turned into a CASPR topic, here's how to start a group and lead a team.

1. **Select a topic.** Check the list of topics at www.caspr.org/list.html. Select the one you're interested in leading. If you see any individual names listed, those are people who may not be interested in leading the group but who've offered to help.
2. **See if a group exists.** Visit <http://www.caspr.org/teams.html> to see if a group has already been organized. If not, this is your chance to be a leader.
3. **Join Yahoo Groups.** If you're a member of the CASPR-Project forum, you already have a Yahoo groups ID. If not, go to <http://groups.yahoo.com/> for instructions on creating a Yahoo ID.
4. **Create a CASPR Yahoo group.** On that same page, about a third of the way down on the right is a link to "start a group". Click that to open up the group creation page, and give your group a name that starts with CASPR-, such as CASPR-Application.

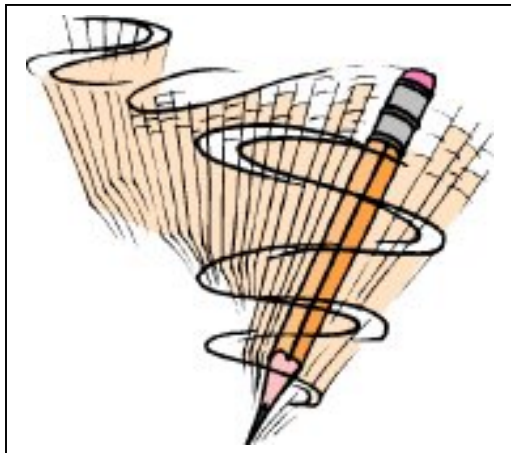


5. **Set joining options.** The series of 2 or 3 screens will give you several options for how you want to administer your group. For example, you can categorize the group so that people can find it based on their interest in the topic (thus far CASPR has been categorizing the groups as IT/Security). Also, you can choose whether to allow anyone to join, or whether you want to approve each request to join - the latter of which gives you a chance to screen people by communicating with them ahead of time if you want. It also creates added overhead for you that you may not want to deal with. If you choose this option be sure that you can be prompt in responding to prospective members.

6. **Invite people to join.** Once you have created the group, you can invite people to join by entering their e-mail addresses. Or you can skip that step and just send a message to the whole CASPR-Project mailing list, letting people know you've set it up and giving them the links to subscribe.

7. **Create a list of potential topics.** Consider putting some ideas together ahead of time, since people tend to focus more quickly with some suggestions than with an open "what should we do?" question.

8. **Decide how to focus your paper.** Once you've got this step done and people start to join, you can start communicating amongst yourselves as to how you'd like to focus your Practice paper. Start with general brainstorming about what topics need to be covered and any bullet points that group members would recommend.



9. **Organize an outline.** Take everyone's recommendations, put them together and organize them into some sort of checklist or outline.

10. **Decide how to write the paper.** Communicate with group members to decide how to research and write the paper. Someone (or several people) should first search to see if "best practices" have already been written on the topic. That will give you clues as to practices that may be commonly accepted already. Later in the newsletter you will find several links to documentation.

11. **Break out the work to team members.** If your topic can be easily divided into discrete sub-topics, consider asking each group member to write a section on that sub-topic. Then, you can collect the sub-topics and integrate them into a whole.

12. **Put the whole paper together.** Another approach would be for someone to write the whole initial paper, and then submit it to the other group members for review and suggestions.

Dealing with Scope Issues

There are several groups that are still in the early stages of “practice-writing”. As they meet (or e-meet) to decide how to address their chosen topics, some are finding it difficult to narrow down the scope of the practice, or to focus on the key points of each topic in order to get started.



Part of the problem is that the topics are very broad. It could take months to cover all of the important aspects of any one of them. Another part of the problem is that most of the practices are intimately entwined with others, and while we're writing advice on the best way to do one task, we naturally want to advise on the best way to do related work. Here is some advice to help keep your papers clear and succinct.

- a) Before fully defining your scope, take a look at the list of topics that can be found at <http://www.caspr.org/list.html>. If your topic is related to another on the list, define your own scope as narrowly as you can and avoid discussing the related topic in detail. If your paper needs to touch on the related topic, just refer to the other paper: “See the CASPR Practice on Windows 2000 Security for additional details”. As the CASPR project matures and more papers get ready for publication, a comprehensiveness review can be done to ensure that we don't wind up with any "dead links".
- b) If the team can't narrow down the paper's topic, write an outline that includes all the aspects you want to cover. Then pick one aspect and start writing the details for just that aspect. Finish discussion of just that part before moving on to the others. You might decide to stop and end your paper there, or to continue with the next aspect. Either way, you'll have covered the ground of something important.
- c) If the chosen topic is closely related to another, consult with the related team, if one has been formed, and see what they think. You might find that they've already covered the ground you're struggling with.



- d) If there are enough team members, think about breaking up into two (or more) groups, each of which can cover a smaller piece of the big topic. Each team can then build their own paper and the two pieces can be merged together at the end.



- e) Consider writing more than one paper, looking at the practice from more than one perspective. For example, the Policy group is creating two papers. One has information targeted at executive staff on how to make policy decisions; the other is looking at the technical aspects of what should be included in a security policy.
- f) Toss the scope issue out to the entire CASPR-Project group for wider discussion. This might generate some new members for the group, and feedback may provide some insight that hasn't been considered yet.
- g) Remember that as CASPR's name implies, the goal is to create a set of recommendations that

are generally agreed upon by a project team that has significant security experience. That means that one of the most important things to do is to keep the paper narrowly focused, cover ground thoroughly, and stay vendor and technology-neutral (i.e. does not apply to WIN/2K type papers). Given the speed with which technology is evolving, no matter how much is written it will never be possible to document *everything* that's important. So it's far better to write something clear and succinct, than to miss something important by trying to cover too much ground.

Life on a CASPR Team (or maybe more than one)

When CASPR got started, Laurie McQuillan volunteered to lead two teams, one on Certification and Accreditation (C&A), and later, one on Information Security Policy. The C&A effort started out quickly, and the group got an initial paper put together within a month or two. The Policy effort was lucky, when one of the members had a paper already written that was to be used for another purpose, and agreed to contribute it as the start for the Policy team.

In the C&A effort, there were constraints brought about by the author's (Laurie's) lack of experience in the commercial world. The initial draft showed a bias towards the civilian government arena. Luckily, three of the team members had extensive experience with C&A work, and the second draft of the paper reflects the extensive comments and suggestions from a team effort

The cycle seems to be that things will then quickly bog down, even with a draft or two put together. Both C&A and Policy groups have lots of members, but most of them are “silent” and seem hesitant to comment or contribute. In both the Policy and the C&A group, there are 3 or 4 active members, and the remainders of the team are only watching in the background. It is like any team effort: you will only get out of the process what you put into it. As the cliché goes, “No information is bad information.”

It is likely that the Team Lead is going to do the majority of the work, with three or four people helping to guide direction and content. When Laurie helped to start the CASPR effort, she assumed that the writing would be a cooperative effort, but it seemed more expedient (at least in the groups that she has participated in) for one person to do the writing, and the other team members to contribute ideas and suggestions.

On your teams, you may want to consider establishing some deadlines, so that you can keep your teams moving forward. If you have suggestions on how to keep a team focused and producing a result, let anyone on the leadership team know so we can publish it for all to use.



CASPR Document Review Process

1. Draft Creation

Work groups are created of any subject matter expert who wishes (or we can coerce) to help. Each team will have at least one CISSP who will act as Draft Editor and will make sure that the draft fits with the style and organization of the rest of the documents. As the CISSP certification requires broad knowledge of InfoSec the editor can also help the groups from becoming too myopic and addressing their topic without regards for InfoSec as a whole.



2. Internal Review (all CASPR members)

Once complete, drafts will be submitted for internal review by other members of the project. Members will make comments, corrections, and suggestions and the working group will revise the document accordingly or justify their content.



3. External Review (CISSP Forum)

Once the Internal review is complete, drafts will be submitted for external review to the CISSP Forum for comments, corrections, and suggestions. The working group will further revise the document accordingly or justify their current content.

4. Public Release

Once the External review is complete, we will publish the documents publicly.

5. Public Review

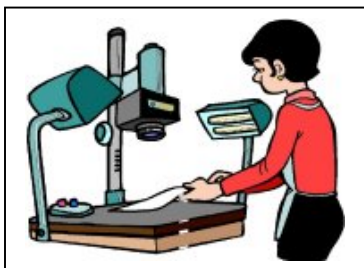
Once published, there will be an easy way for the public to make comments, corrections, and suggestions as the document is put to use.

6. Addendums Released

The working group will take these comments and suggestions and submit addendums to the published document as needed.

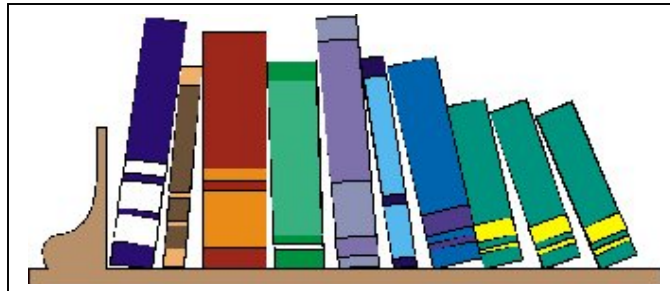
7. Revise, review, & republish

Every 6 months the working group will go back to step one and revise the document to include the addendums and other improvements. This new draft will be put through the review process again.



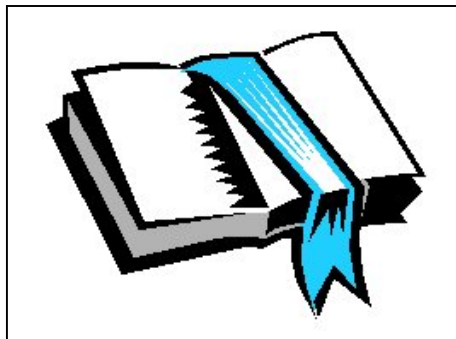
Links to other Documentation and “Best Practices”

Many of the topics on our CASPR list of recommended practices have been addressed before, or have been touched on by other Best Practices papers. Here are some links to check out when doing research on your papers. These links can also be found on the CASPR web site at www.caspr.org.



PRACTICE NAME	INTERNET ADDRESS
Arthur Andersen Global Best Practices	http://www.globalbestpractices.com/Topics/Subtopics/default.asp?N=T,273,09
Best Practices and Guidelines	http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14_tax281901,00.html
Best Practices for Digital Archiving	http://www.dlib.org/dlib/january00/01hodge.html
Best Practices for Nokia WAP Server Security	http://www.symantec.com/avcenter/security/Content/2000_07_17.html
Best Practices for Secure Web Development	http://www.itsecurity.gov.in/general_security/web_security/best_practice1.htm
Best Practices for Seizing Electronic Evidence	http://www.theiacp.org/pubinfo/pubs/bestpractices.htm
Best Practices in Internet Security	http://www.more.net/security/best.html
Best Practices in Managing World Wide Web Server Security	http://ciac.llnl.gov/ciac/bulletins/j-042.shtml
Best Practices in Network Security	http://www.networkcomputing.com/1105/1105f2.html
CERT® Security Improvement Modules	http://www.cert.org/security-improvement/
CERT® Security Practices	http://www.cert.org/nav/index_green.html
Data Protection Best Practices	http://www.dlftape.com/education/bestpractices/
Deploying Windows 2000 with IIS 5.0 for Dot Coms: Best Practices	http://www.microsoft.com/windows2000/techinfo/planning/incremental/iisdotcom.asp
Enterprise-wide Information Security Policy Best Practices	http://www.security-informer.com/english/crd_information_321966.html

PRACTICE NAME	INTERNET ADDRESS
Establish policies and procedures for responding to intrusions	http://www.cert.org/security-improvement/practices/p044.html
Generally Accepted System Security Principles (GSSPs): Guidance on Securing Information Technology Systems	http://csrc.nist.gov/publications/nistbul/csl96-10.txt
Guide to the Selection of Anti-Virus Tools and Techniques	http://csrc.nist.gov/publications/nistpubs/800-5/800-5.txt
Guideline for Implementing Cryptography in the Federal Government	http://csrc.nist.gov/publications/nistbul/itl00-02.txt
Guidelines on best practices for using electronic information	http://europa.eu.int/ISPO/dlm/documents/guidelines.html
Information Security Risk Assessment: Best Practices of Leading Organizations	http://www.gao.gov/special.pubs/ai00033.pdf
Information Warfare and Information Security on the Web	http://www.fas.org/irp/wwwinfo.html
Internet Best Practices Standards Working Group	http://www.computer.org/standards/Internet/
Links to ISS Practice Publications	http://www.auerbach-publications.com/iss/
Management of Risks In Information Systems: Practices of Successful Organizations	http://csrc.nist.gov/publications/nistbul/itl98-03.txt
NT Security Best Practices Team	http://www.wisc.edu/arch/teams/nt_security/best_practices/nt_sec_best_practices.html
Privacy Compliance Resources Best Practices	http://www.idcide.com/pages/res_best.htm
Protecting Your Laptop Computer	http://www.itso.iu.edu/howto/laptop/
Public-Key Cryptography Standards	http://www.rsasecurity.com/rsalabs/pkcs/



PRACTICE NAME	INTERNET ADDRESS
Security Best Practices for Internet Service Providers	http://www.icsa.net/html/communities/ispsec/downloads/Best_Practices_v6.%20rev.rtf
Topics on Computer Security	http://www.epic.org/security/
Topics on Cryptography	http://www.epic.org/crypto/
Topics on Privacy	http://www.epic.org/privacy/
Web Security	http://webdeveloper.earthweb.com/websecu/archives/
Web Site Administration Policies & Procedures	http://resnavy.spawar.navy.mil/dod.html

Summary

If you have some success stories in preparing your papers or tips that others can use, send them to any member of the CASPR Leadership team so we can include them in a future newsletter.

Should you have any questions or wish to get more information, please don't hesitate to contact any member of the team:

Bob Johnston: bjohnston@e-computer-security.com

Ken Shaurette: KShaurette@home.com

Laurie McQuillan: LMcQuillan@Hill-Clan.org

Thomas Akin: takin@crossrealm.com

Curt Vonancken: Webmaster@caspr.org

