

## Fwd: Oh Dear, Where to start?!

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-06/0873.html>

---

**From:** Rick Jones ([rwjones2001\\_at\\_hotmail.com](mailto:rwjones2001_at_hotmail.com))

**Date:** 06/26/03

To: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

Date: Thu, 26 Jun 2003 18:56:17 +0000

Believe it or not, I really envy you. There's nothing like a total mess to clean up to teach you something. You know, experience is the best teacher yada yada yada.

It seems to me you need two things: an organizational policy, and a plan. Here's how I would approach it...

Since it is a government office, you are undoubtedly part of a hierarchy. So the first place to start is at the top. All governments -- be they federal or state -- have top-level policy documents stating what is required. So begin by finding that ur-document. As you move down the hierarchy, you will find lower-level documents that give more detail and provide more specific guidance. As a general rule, you can make your own organizational policy more stringent than the ones above it, but not less stringent. So developing a policy should be relatively easy: find the policy of the next echelon up, and adapt it to your own unique needs. Remember: policy is policy, it is not a technical specification.

The organizational policy you develop will surely take time to get approved, but in the meantime, you have the policies of the upper-hierarchy that don't need any approval at all -- they are already approved. Therefore, they are requirements, and you can use them to develop a plan.

Examine your requirements documents and try to discern the categories of usage. If you are dealing with the federal government, for instance, the operative phrase is "information assurance," and the relevant categories are: confidentiality, availability, integrity, non-repudiation, and a few others. You should phrase everything in terms of the relevant categories of usage from here on out.

With requirements in hand, do a baseline assessment. By that I mean, state what your organization has in place using the vocabulary and (hopefully) metrics from your requirements documents. Again, you should not be talking technologies at this point (unless your requirements documents do. If they do, they are flawed, but that's another issue.)

Having assessed your current state of affairs against the requirements, you

## SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

now have a delta, or difference between what's required and what's currently present.

Next, try to determine the resources required in each category of requirement to fill the delta; i.e., to get from where you are to where you need to be. Generally, resources are expressed in terms of time, money, and/or people (manhours). At this point you introduce technical solutions if appropriate.

From that, create an "impact statement" for each category that clearly states all the bad things that could happen if the requirement is not filled. As an aside, you will probably need a threat assessment to do this.

Present that entire thing to your boss: what's required, what's missing, what it will take to get each category to where it needs to be, and the impact of not doing it. Then ask him or her to prioritize.

If you get that far in three months, consider yourself a success and your time well spent. My guess is that you won't even get close to getting your hands dirty with firewalls, encryption, passwords, etc. Those are all details that come later. But don't worry about it, you'll have plenty of time to do that kind of stuff once you finish college. In the meantime, not everyone has the opportunity to grapple with the sort of high-level stuff facing you. It might not be as enticing as setting up firewalls or whatnot, but I can assure you that if you do it slowly, methodically, and well, you will have a depth and breadth of experience that'll be worth gold.

Once again, it's really an enviable situation for someone getting ready to finish college and break into the real world of computer security. It'll be a great experience. Good luck.

N.B., I would be very interested to hear from you at the end of the summer. What you tried, how it was received, how far you got, etc.

–RWJ

Hey everyone,

Ok... I am in a bit of a jam here and I was hoping to get some feedback from some of you with appropriate experience in the field of network security and policy development.

I am an senior at RIT studying (essentially) systems administration. My main focus and priority has been computer security and policy development. I recently took a internship with a small government office helping out with computer administration tasks. Upon arrival, I decided it would be fun to do a windows update to see what sort of things would come up for my PC. Low and behold, there were over 40 critical

Fwd: Oh Dear, Where to start?!

## SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

updates, driver updates, and recommended updates.

Right off the bat this triggered the feeling that there was absolutely no security or update plans in place at this particular organization. I quickly addressed the issue, and have been working to draft a comprehensive security policy and implement technical controls.

What I need advice on is the following: If you were introduced to a mixed network (literally all versions of windows since 3.1 and mac systems) that have no updates, backups, or patches installed... connected to a network with only a basic NAT table and no other security... with not even anti-virus software enabled... with no user policies or disaster plans in place... with unprotected netbios shares everywhere... where would you start the process of building some sort of security solution?

I mean, I've seen passwords on monitors, shared accounts, open public ports (even the wiring cabinet was unlocked in plain view of passbys to the building). I've been tasked with creating the security policies relating to internet use, network and phone use, passwords, physical security, backup/disaster plans, antivirus, incident response, email use/protection, and whatever else needs done. This wouldnt be so bad normally I guess, but there is virtually no budget allocated to help for this project and I have approximately 3 months to do it. To make matters worse, I am also responsible for systems admin, network admin, tech support, programming, and whatever other tasks may need to be done in the meantime.

So basically, if you had to start from nothing, where would you start first? What would you consider to be the most important things to be implemented? I am literally working from ground zero here... heh!

Thank so much in advance ;-)

Steve Frank

---

President SPARSA  
Security Practices and Research Student Association  
Rochester Institute of Technology

## SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

---

Do you Yahoo!?  
SBC Yahoo! DSL – Now only \$29.95 per month!  
<http://sbc.yahoo.com>

---

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant,  
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug–n–play secure remote access in  
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

---

Believe it or not, I really envy you. There's nothing like a total mess to  
clean up to teach you something. You know, experience is the best teacher  
yada yada yada.

It seems to me you need two things: an organizational policy, and a plan.

Since it is a government office, the first place to start is at the top.  
All governments have top–level policy documents stating what is required.  
Generally from there you will find lower–level documents that give more  
detail and provide more specific guidance. All of these are the  
requirements you need to work against, and as a general rule, you can make  
your own organizational policy more stringent than the ones above it, but  
not less stringent. So developing a policy should be relatively easy: just  
the next echelon up's policy, and adapt it to your own unique needs.

Now you need a plan.

Once you have your requirement (i.e., policy) documents identified, do a  
baseline assessment. By that I mean, your requirements documents should  
have given you the vocabulary and (hopefully) the metrics for what's  
required. So — using that vocabulary and those metrics — state what is or  
is not in place at your organization.

Now you have a delta, or difference between what's required and what's  
currently present.

Next, try to determine the resources required in each category of  
requirement to fill the delta; i.e., to get from where you are to where you  
need to be. Generally, resources are expressed in terms of time, money,  
and/or people (manhours).

Next, create an "impact statement" for each category that clearly states all  
the bad things that could happen if the requirement is not filled.

## SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

Finally, present that entire thing to your boss: what's required, what's missing, what it will take to get each category to where it needs to be, and the impact of not doing it. Then ask him or her to prioritize your tasks.

Finally, remember that security generally rests on three things: people, policies, and technologies. Don't just focus on one thing and lose sight of the others.

Once again, it's really an enviable situation for someone getting ready to finish college and break into the real world of computer security. It'll be a great experience. Good luck.

Hey everyone,

Ok... I am in a bit of a jam here and I was hoping to get some feedback from some of you with appropriate experience in the field of network security and policy development.

I am an senior at RIT studying (essentially) systems administration. My main focus and priority has been computer security and policy development. I recently took a internship with a small government office helping out with computer administration tasks. Upon arrival, I decided it would be fun to do a windows update to see what sort of things would come up for my PC. Low and behold, there were over 40 critical updates, driver updates, and recommended updates.

Right off the bat this triggered the feeling that there was absolutely no security or update plans in place at this particular organization. I quickly addressed the issue, and have been working to draft a comprehensive security policy and implement technical controls.

What I need advice on is the following: If you were introduced to a mixed network (literally all versions of windows since 3.1 and mac systems) that have no updates, backups, or patches installed... connected to a network with only a basic NAT table and no other security... with not even anti-virus software enabled... with no user policies or disaster plans in place... with unprotected netbios shares everywhere... where would you start the process of building some sort of security solution?

I mean, I've seen passwords on monitors, shared accounts, open public ports (even the wiring cabinet was unlocked in plain view of passbys to the building). I've been tasked with creating the security

Fwd: Oh Dear, Where to start?!

SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

policies relating to internet use, network and phone use, passwords, physical security, backup/disaster plans, antivirus, incident response, email use/protection, and whatever else needs done. This wouldnt be so bad normally I guess, but there is virtually no budget allocated to help for this project and I have approximately 3 months to do it. To make matters worse, I am also responsible for systems admin, network admin, tech support, programming, and whatever other tasks may need to be done in the meantime.

So basically, if you had to start from nothing, where would you start first? What would you consider to be the most important things to be implemented? I am literally working from ground zero here... heh!

Thank so much in advance ;-)

Steve Frank

---

President SPARSA  
Security Practices and Research Student Association  
Rochester Institute of Technology

---

Do you Yahoo!?  
SBC Yahoo! DSL – Now only \$29.95 per month!  
<http://sbc.yahoo.com>

---

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant,  
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in  
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

---

The new MSN 8: smart spam protection and 2 months FREE\*  
<http://join.msn.com/?page=features/junkmail>

---

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant,  
while InStat has confirmed Neoteris as the leader in marketshare.

Fwd: Oh Dear, Where to start?!

## SecurityFocus BASICS: Fwd: Oh Dear, Where to start?!

Find out why, and see how you can get plug-n-play secure remote access in about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

---