In a closed discussion group to which I belong, a member posed the following interesting problem. The participant has very kindly allowed me to publish the conversation with some details changed to preserve anonymity.

* * *

[The member started the discussion as follows:]

In the past I have asked how information assurance in positioned within your organization. In some, IA is a part of operations, in some it is the same people doing both IA and operations, some organizations have IA teams that act as internal consultants to operations, and some have IA operations that work along side production operations.

I have a question in a similar vein. For those security functions that require administrator privileges, do your IA personnel have either Local or Domain Administrator accounts? We are debating a philosophical issue here where our requests to be granted local admin privileges on servers are denied, but the subsequent requests we make of the people that have admin privileges to do the work we are unable to perform go unanswered. Essentially we are in a position of not being able to perform certain tasks related to security, and we are not getting cooperation from the production support teams. We wonder if security personnel at other organizations are given administrator accounts or not.

* * *

[I responded with these comments:]

I think the critical element here is as follows:

>…[O]ur requests to be granted local admin privileges on servers are denied, but the subsequent requests we make of the people that have admin privileges to do the work we are unable to perform go unanswered.<

In a production environment, distributing administrator privileges may disrupt production controls, so I can understand the desire to centralize the administrator functions to a group of people who work closely with others within the production team.

However, assigning responsibilities without authority is never good.

I think that you should explore and analyze the roots of this breakdown in communication between your group and the production team that is supposed to be (but isn't) supporting you. Has the rift developed recently or is it historical? Are there specific personal conflicts that may
account for this division between the teams? Are their conflicts between the managers of these groups? Do the obstructive personnel understand the requests and their urgency? Are they perhaps overworked and therefore assigning lower priority than they ought to in scheduling responses to specific requests?

By focusing on the underlying organizational dynamics here, you may be able to present a recent case to your manager so that he or she can take appropriate action to resolve the problem constructively.

But simply pointing how other organizations handle the assignment of administrator privileges is, in my experience, unlikely to get you very far.

* * *

[The participant elaborated on the situation:]

> Distributing administrator privileges may disrupt production controls<

I worked for several years as a systems administrator before specializing in security, so I completely agree. In fact, I do not _want_ administrator privileges unless I absolutely need them.

> Has the rift developed recently or is it historical?<

Historical. The Security department at my organization, historically, is staffed by very non-technical people. Until recently, Security did not engage in technical activities. Therefore, the department has always been viewed by the technical staff as technically incompetent. To be frank, in some cases, this is true.

> Are there specific personal conflicts that may account for this division between the teams?<

Yes. I worked with the operations folks for several years before switching teams. I like to think that I get along with them fine, if for no other reason than the fact that I have walked in their shoes. The specific two individuals that want local admin access have never worked in a production support environment, so they have a hard time earning the admins' trust.

> Are there conflicts between the managers of these groups?<

Sadly, yes.

> Do the obstructive personnel understand the requests and their urgency?<

I believe so.

> Are they perhaps overworked and therefore assigning lower priority than they ought to in scheduling responses to specific requests?<

Very likely. I had gone so far as to suggest, in writing, that we form an operational security group to take on the tasks that production support cannot make time for. The new group would
be independent from the internal consultancy security group to maintain proper checks and balances, and staffed by personnel with the appropriate skills. This idea has garnered limited support so far.

I'll suggest that my organization explore the social dynamics rather than focusing only on the technical and see how that goes. I'd also welcome any comments on the idea of having two security teams – one that has an audit function, and one that has a technical function. I realize that this idea has flaws, but I think it has benefits as well.

[MK adds: I am always in favor of having a separate audit function if at all possible. The nature of audit is inherently better supported with an independent reporting structure than if the auditors report directly to the managers of those being audited.]

As a final note in this interesting discussion, my correspondent sent me the following encouraging note several weeks after the exchange above:

> You'll be glad to know that as a result of it, leadership from the security and operations groups (including management and technical staff) now meet regularly. We hope to foster better working relationships and communication. We've only had a handful of meetings so far, but everyone agrees it is in the organization's best interest if the two teams work together, as opposed to against one another. Progress! <

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.