

# Security: Beyond Technical Measures

## Steps toward a comprehensive information security policy

*Linux folks tend to have a better eye on security. I realize that's an overwhelmingly general and wide-sweeping statement, but that's my opinion. I've been working with Linux for a very long time, and most of the other users in the community tend to be highly technical and thus aware of many of the security concerns facing the networked world today. And let's be honest, there's a reason we all choose to use an open source operating system that allows direct access to the kernel source code and its modules.*

Linux allows us to build robust firewalls, intrusion detection, and file system integrity checkers. The firewall I've installed at my own company is based on a Slackware 9.1 iptables implementation. The Linux world has provided us with forensic tools, vulnerability scanners, network analyzers, and more. I can now test my network, scan for security issues, resolve those issues, and investigate potential compromises, all from the comfort of my shell prompt.

Not only do these tools provide the ability to secure my organization at a fraction of the cost of the more commercially based tools, but they also let me see what they're doing. They have nothing to hide. In the end, I can know everything I want to know about my own security.

But let's step away from the technical aspects of security for just a moment. The Linux community has been great at addressing our technical problems, but it's missing another piece of the puzzle that simply cannot be addressed by software: the organization itself. Organizations need to have the underlying policies, procedures, and culture associated with security or else it becomes a simple matter of "user = bad password" or "screen = unlocked" and all of our network security measures have been compromised.

Coming from a technical background myself, this was the hardest nut for me to crack. Dealing with policies and procedures was always something that managers were supposed to do. I don't do policies. But it occurred to me in a moment of great enlightenment (OK, I'll admit it, it was actually over a Mountain Dew and a Soft Taco Supreme) that most managers can't understand the security side like many technical people can. So who's going to translate reality into potential policies for the managers? In the end, it falls to those technical individuals willing to take up the banner of information security and endure the pains of policy and management.

The National Security Agency (NSA) developed a system, years ago, called the INFOSEC Assessment Methodology (IAM) that can be used to conduct assessments against the organizational side of each company. The system doesn't deal directly with the technical side of security assessments but instead strives to answer questions about organizational policy, procedure, and culture. The IAM is based on the very same procedures that NSA uses to assess the security of military and federal sites all around the world.

The IAM is used to determine the actual security posture of an organization based on how it addresses security within its policies and procedures. What's actually covered within the organizational security policy? What's missing? Are any of these things actually enforced? How? What security regulation is our organization required to adhere to?

The IAM breaks down this analysis into three phases: the Pre-Assessment phase, the On-Site phase, and the Post-Assessment phase. The Pre-Assessment phase consists of activities that try to get the customer to sit down and decide what information is critical to the organization's business. The goal is to get the customer to start thinking in terms of confidentiality, integrity, and availability. We start by getting customers to ask themselves questions like "What is the impact to my organization if I lose integrity of these customer records?"

In most cases, these decisions have to be made by upper management-level personnel who understand the ins and outs of the business process. But what the IAM delivers at the end of this phase is an easy-to-read matrix that lists the most critical information types along with the customer ratings for the impact each one would have on the organization if it were compromised.

One of the most useful aspects of the IAM is that it also gets the customer to sit down and list the specific systems within their own networks that contain each of these critical pieces of information. So now we know which information is critical to the organization, what impact it would have on the organization if we had a compromise, and where that information exists. This provides a great starting point for technical assessment activities because the customer has identified the most critical servers and network components.

The On-Site phase is used to verify policies and regulations and to determine the actual level of adherence to these things. The activities include documentation review, interviews, system demonstrations, and review of network documents. The NSA IAM has worked with the National Institute of Standards and Technology (NIST) to generate a list of areas that are covered during these activities. These areas are broken into three areas: Management, Technical, and Operational.

Management:

- INFOSEC documentation
- INFOSEC roles and responsibilities
- Contingency planning
- Configuration management

Technical:

- Identification and authentication
- Account management
- Session controls
- Auditing
- Malicious code protection
- Maintenance
- System assurance
- Networking and connectivity
- Communications security

Operational:

- Media controls
- Labeling
- Physical environment
- Personnel security
- Education training and awareness

As you can see from the list above, the IAM allows for a complete organizational assessment while still allowing for the flexibility of customization for each independent organization.

Finally, the Post-Assessment phase is generally used for creating recommendations for areas that are not being addressed appropriately and could lead to an impact on the business. With the appropriate management buy-in at this point, the final report that is produced in the Post-Assessment phase can be used as a roadmap for the organization to an increased security

posture. The management buy-in is especially vital when we consider the significant cultural and policy change that should occur in response to an assessment process of this magnitude.

I think we all agree that great technology is a wonderful thing, but if we stop and really analyze the entire situation, we find that we need both sides of the puzzle if we're to have the best security possible for our organization. Using a methodology like the IAM can help your organization take the next steps toward a comprehensive information security program and augment your technical measures. For more information on the NSA IAM, please visit [www.iatrp.com](http://www.iatrp.com) or [www.securityhorizon.com](http://www.securityhorizon.com).