Herding Cats 101:
Development & Implementation of Security Policies at a University

Jodi Ito
Security Essentials Practical

As the owner of two cats, I can vouch for the fact that trying to get a cat to do anything on command is akin to making water flow uphill. Nearly impossible! Just like getting faculty, staff and students to readily agree to and abide by a university's security policies. And that would be only half the battle. The other half being the creation and adoption of such security policies.

Universities have a well-deserved reputation for being primary launching sites for computer and network attacks. The "open" environment of a university lends itself well to the development and promotion of research and learning activities of faculty and students. But these same features make the university an ideal playground for the less well-intentioned. One of the launch points in the series of denial-of-service attacks in February 2000 was a university in California. The system used to launch one of the attacks was compromised from a source outside the university.

These widely-publicized “hacker” incidents showcase the need for a basic security policy which governs and oversees the type of activities that are allowed on university computing and network resources. By providing basic guidelines for responsible and ethical use, a valuable resource can be shared by all university community members without infringing on the rights and privileges of others but still allowing enough flexibility and freedom for everyone to accomplish their goals and objectives. Without a policy in place, it is impossible to restrict undesirable activities.

Development of security policies

In any organization, either private or public organizations, it would be difficult to have a single document be the authoritative SECURITY POLICY. Generally, multiple documents are needed to cover the broad range of issues and activities that fall into the category of “security”. Separate policies should address different issues such as “Acceptable Behavior and Responsible Use”, “Administrative Information Systems Security Policies”, “Guidelines for Server Configuration and Attaching to a Network”, “Software Security Policies”, “Securing of Confidential Data”, etc. Additionally, security policies in a university environment have to encompass and allow for a broad range of activities.

But each policy should include (where appropriate) the following components:
- reasoning behind the creation of the policies
- expected and allowed behavior and activities

- individual roles and responsibilities
- ownership, disclosure, and confidentiality of systems, resources, and data
- due process and
- penalties and severity of penalties for any violations or infringements.

Wherever possible, these security policies should reference existing policies to leverage processes already in place as, many times, technology just provides a different media and additional opportunities for behaviors already addressed elsewhere. For example cheating and plagiarism are already addressed in Student Code of Conduct policies. The medium by which the behavior is executed should not supercede the behavior itself. Harassment is still harassment whether done face-to-face or electronically through email.

Additional supporting documents may address technical issues such as detailed instructions for securing specific systems and services, software installation and configuration, password administration and management, guidelines for attaching servers to the central network, backup policies and management, etc.

Prior to developing these policies, it is important to assess what resources need to be protected and to determine what CAN be protected. There's no point creating a policy or rule that cannot be enforced. It is also helpful to review policies of other institutions and organizations as almost everyone has to deal with these same issues. It's often beneficial and insightful to look at different viewpoints and philosophies from organizations with various purposes and goals.

Who should develop these policies?

If possible, recruit a task force comprised of representatives from different populations of the university community to develop these security policies. The committee should include representatives from faculty, faculty administration, students, staff, system and network administrators, technology support staff, and especially university administration. While the process may take more time, the end result will be a greater acceptance of these policies by the members of the university. And it is crucial to gain the approval and support of university administrators otherwise the ability to implement them will be severely curtailed.

Release initial drafts as Interim policies.

Releasing an earlier version of the policies allows you to "work as you go". You retain the ability to fine-tune the policies before actually soliciting the formal approvals necessary for adoption. The process and effect of the interim policies can be monitored to see if the desired results are achieved. It may turn out that some of the recommendations may be too onerous or labor-intensive to put into practice. During this time, it would be prudent to solicit comments and opinions from larger populations such as student organizations, executive and administrative committees, technical support organizations, and faculty and staff unions.

Once the revision process has been completed, the final version should be compiled and re-released for final comment.

Formal adoption of the policies does not signal the end of this process. In fact, nothing could be further from the truth. Having a policy in place, does not indicate that everyone will know about it and that it will be followed by everyone. There must be some way of notifying and educating the university community of the importance of abiding by these policies because without the underlying understanding, it will be like herding cats – nearly impossible at best. And this is only the beginning of an on-going, continuing process.

We have policies, now what?

The university community needs to be made aware of the existence of your security policies and the impact of their negligence to abide by those policies. Security is not just a set of documents and policies, but it's a mindset and philosophy that needs to be embodied by all. As we all know, the strength of our security is as strong as our weakest link. All members of the university need to understand their roles and the importance of their unified participation.

Implementation of security policies can be tackled with a multi-pronged approach:

- education and awareness campaign
- development of implementation recommendations and specifications
- on-going training opportunities for technical support staff
- monitoring and tracking of incidents
- continual review and modification of policies

Formal adoption of the security policies by the university should be prominently and widely announced in both official notification channels as well as informal casual forums. Face-to-face group meetings may be held to explain the reasoning and impact of these policies and on-line forums may be used to carry-on discussions electronically. The more opportunities provided for the community to learn about these things, the wider the adoption and support of these security policies.

The technology support organization for the university can assist in the implementation of policies by developing specific guidelines and recommendations that provides step-by-step instructions that end-users can follow. This translates the more general policies into specific actions items that are easy to put in practice.

Training of support staff provide the opportunity to indoctrinate the "security philosophy" into those that are directly involved and responsible for assisting the end users. This train-the-trainer philosophy leverages an existing information distribution structure to facilitate getting the word out. By teaching security strategies and practices to support staff, they can ensure their end users are actually using them.

Monitoring, coordinating, and tracking of security incidents allows you to see if your security policies are actually helping to decrease the number of incidents that are occurring on your campuses. Or you'll be able to see if any changes need to be made to your policies. Without an incident tracking process, you cannot determine the impact the policies is having, for better or for worse, on your organization. It doesn't make any sense to have policies in place that doesn't improve the situation.

And finally, security policies and procedures must be reviewed constantly. Technologies change, threats change, risks and vulnerabilities change. To ensure that our policies still meet our needs, an on-going review process must be adopted. Otherwise, we'll be right back to square one.

References:

Hopper, D. Ian, Thomas, Pierre, "Consulting firm says its server was used to attack AOL", 11 February 2000, URL: www.cnn.com/2000/TECH/computing/02/11/cyber.attacks.01/index.html , (21 November 2000).

University of Hawaii, "Use and Management of Information Technology Resources", October 1999, URL: www.hawaii.edu/infotech/policies/itpolicy.html, (22 November 2000)

University of Virginia, Information Technology and Communications, "Security Policy", 1 September 1994, URL: http://www.itc.virginia.edu/policy/Policies/security.html, (21 November 2000).

U.S. Department of Education, National Center for Education Statistics, *Safeguarding Your Technology*, NCES 98-297, Washington, D.C.: 1998

Virginia Polytechnic Institute and State University, "Acceptable Use of Computer and Communication Systems", 4 June 1999, URL: www.vt.edu/admin/policies/1000/2015.html, (22 November 2000)

Virginia Polytechnic Institute and State University, "Acceptable Use Of Information Systems At Virginia Tech", 16 June 1999, URL: www.vt.edu/admin/policies/acceptuseguide.html, (22 November 2000)

Wood, Charles Cresson, *Information Security Policies Made Easy*, California: Trade Services Publications, 1997