

Opening Eyes: Building Company-Wide IT Security Awareness

Mark McGovern

Managing IT system security is a never-ending effort. Regardless of how well you secure a system today, new threats and issues will appear tomorrow that will send chills down the IT manager's spine. User support, IT staff enthusiasm, and management buy-in are critical assets for overcoming the constant barrage of threats. Unfortunately, there is no standard playbook that tells IT managers how to manage these relationships and focus them on security issues. Every IT staff must build its own strategy.

Various organizations have successfully used the following concepts to manage security. This list serves as a good source of ideas for how IT managers can use awareness to advance their security goals.

PRACTICE WHAT YOU PREACH

An IT staff interested in security should set an example for the organization. Establishing internal policies for incorporating security into IT projects is an easy method of ensuring that the actions of the IT staff demonstrate support for security. Depending on the organization's sophistication, these policies may define simple technology standards or review processes or user interfaces. However, regardless of an organization's sophistication, IT



Security awareness is key to keeping systems safe. Small changes can move security higher on your user group's radar screen.

project policies should ensure that everyone addresses security consistently. Such consistency reduces the amount of IT resources required to train users and also reduces the conflicts that arise when users must interact with disparate systems.

IT'S HARD TO BE WRONG WHEN THERE IS NO RIGHT

Security policies define acceptable behavior, expected practices, and responsibilities for an organization. Without written policies, users and administrators are left to decide important issues for themselves. It is surprising how many times an ugly incident reveals that an organization has no policy on a specific security issue. Policies

should clearly assign responsibilities to users, managers, and administrators. In this way, no party can mistakenly assume that someone else is responsible.

IT managers should ensure that policies do not foster fascist acts by the IT staff. Legend has it that IT staffs have been known to lose touch with the big picture and enforce IT policy with a ferocity that secret police would envy, implementing the modern equivalent of ritual beatings, public humiliations, and crucifixions—all in the name of policy. IT managers who are updating policies or reenergizing their use should remain cognizant of this history and ensure that IT staffers remain on friendly terms with their patron users.

TAKE IT FOR A TEST DRIVE

Providing users and managers with demonstrations of technologies and tools can greatly enhance their appreciation of security measures. It significantly magnifies the demonstration's value to highlight an issue of immediate concern to the audience. For example, demonstrating a simple password-cracking system to an audience of new users or to the managers evaluating the new password policy can immensely enhance the chances that strong passwords will be accepted and used.

NOW HEAR THIS

IT staffers can maintain awareness by providing their user community with regular updates on technology threats and security issues. However, IT staffers should take care to ensure that these notices do not become regular spam. Additionally, IT managers should review user notices to ensure that they do not accidentally encourage users to actively try out the techniques or attacks discussed.

WHAT'S MINE IS MINE

Privacy is a serious legal issue for many companies these days. Developing a corporate privacy policy that clearly states the organization's intentions can be useful in building support for security—particularly when the policy's presentation clearly relates how security measures protect user privacy.

Until recently, most companies maintained policies that provided no accommodation for user privacy. Claiming all resources, data, and network activity as assets of the company, such policies often receive serious scrutiny and foster user skepticism. As privacy becomes an increasingly more important issue, IT staffers are beginning to realize that any accommodation they make for user privacy can significantly soften resistance to new policies and generate support for ongoing activities. Farsighted IT staffers have developed policies stat-

ing that the corporate goal is to preserve individual privacy. These policies stress that the company will not implement measures targeted at individual employees—such as e-mail monitoring and file reviews—lightly. A company should resort to such measures only after some indication of nefarious activity or because of a need to protect the company's assets from a specific, identified threat.

PRACTICE MAKES PERFECT

Developing and enhancing the IT staff's skills and experience is an

Providing opportunities to explore the latest hacker and security tools is a great way to reward and encourage an IT staff.

important goal for any IT manager. Providing opportunities to explore the latest hacker and security tools is a great way to educate, reward, and encourage an IT staff. IT managers who provide their staffs with these types of opportunities are often rewarded with innovative and timely solutions to problems. Indeed, the exercises will often discover latent issues in the existing system that the IT staff should address. Some IT organizations encourage or require participants in these efforts to help distribute information about their discoveries to others by delivering presentations or demonstrations.

Clearly, employees provided with this type of opportunity will need to follow a well-defined set of guidelines to ensure that they do not inadvertently compromise the organization's (or someone else's) system. Nefarious use of any technology must be strictly forbidden, and an effective security policy should discourage importing software from unknown sources. In an effort to mitigate risk, organizations can set up stand-alone systems for testing dubious code and ensuring

that everyone understands policies regarding technology use. These caveats may seem severe, but they will not significantly reduce the benefit of the activities. It is always surprising to see how much information techies can find when they are provided the opportunity and encouragement to explore.

WATCH WHAT YOU'RE DOING

Operations, particularly security operations, must provide feedback that lets the organization monitor activities and status. Without monitors, an organization is unsure of whether a process or system is operating properly. Savvy managers will use feedback to ensure management recognizes the IT staff's successes, and to justify resource requests. Ideally, the organization incorporates monitors into every system and activity before deployment.

The specific form that a monitoring capability takes depends on the nature of the system and the reporting goals. Networks, for example, will often produce feedback generated by intrusion detection systems (IDSs), network monitoring, and load management systems. Software maintenance activities can generate reports detailing the utilization of various applications, the present state of the organization's versions, and the pros and cons of upgrading. Web-based systems can implement periodic penetration-testing practices and system inspections. Staff training activities and configuration management efforts can include random inspections of operational systems. You could also configure router and LAN (local area network) systems to produce log reports that highlight issues and trends.

Be careful to focus monitoring mechanisms on issues of importance to the overall system. It's remarkably easy to become inundated with reports and data, and lose the ability to recognize which issues and systems truly need attention. IT managers must ensure

that they delegate responsibility for detailed analyses to the appropriate technical persons. Managers should instead gather information from easily generated summary reports that highlight issues and reporting status. These reports help IT managers to remain aware of security issues, identify weaknesses, and focus resources.

SAY IT AGAIN (AND AGAIN AND AGAIN)

Perhaps the most valuable practice an IT manager can adopt is providing management with regular reports that highlight the current state of security and demonstrate the need for any required resources. By providing management with updates that use monitoring activities such as IDS system reports and software patch issues, an IT manager can ensure that corporate decision makers remain aware of security.

IT managers interested in fostering security awareness will often dedicate

specific sections of regular status reports to security. Such a security section should incorporate the system status, identify weaknesses or risks, and reference activities or resources that could mitigate the risk. Adding these items to regular reports lets managers see the issues and the potential solutions.

TRY IT—YOU'LL LIKE IT

I encourage IT managers to regularly try new things. Too often, IT managers and their staffs settle into a familiar, albeit hectic, routine that looks something like the following:

1. Provide user services.
2. Address management issues.
3. Put out fire.
4. Rinse.
5. Repeat.

If this routine is really working for the organization, that's great. But if not, try something new. One basic com-

puter security assumption holds: There is always someone out there who is faster, smarter, or better equipped than you. Staying ahead of these mythical geniuses—or at least not falling too far behind—requires constant evolution. Encouraging new ideas and creativity as part of your regular routine can help an IT staff keep current. It also has the added benefit of improving employee retention.

Managing security is a constant challenge that can easily overwhelm an IT manager. The ideas presented here illustrate how to focus a wide variety of tasks on security and provide assistance to the IT staff. IT managers should consider adding some of these ideas to their playbook. ■

Mark McGovern is director of software security for Cigital in Dulles, Virginia. Contact him at mmcgover@cigital.com.

IEEE

IT Portal

Stay ahead of the curve

Get the best of the IEEE Computer Society's peer-reviewed, IT-related content all in one interactive community. Read articles, post comments, create polls, exchange ideas and information.

Visit the IEEE IT Portal today

ieeit.mindcruiser.com

