As I mentioned in my last column, I am presenting three articles (this is #2) based on the work of some of my graduate students during class discussions in a course on computer security incident response team management (CSIRTM). What follows is another edited segment based on a summary written by students Mani Akella and Rick Tuttle. Today’s topic is help-desk (HD) software.

* * *


However, cohort members reported many issues with Remedy that make using it difficult at times. Part of the problem seems to be the number of interface options available for the product – normally a Good Thing. Some Remedy implementations lack a Web interface, limiting end-user input. Other postings decried the lack of an efficient graphical user interface (GUI) design; organizations have to customize their installation to fit their individual needs. One can interpret a lack of an efficient GUI design coupled with the capability to customize as both a feature and a flaw. It is a valuable feature because that BMC is responding to the wide variation in individual organizations’ needs: it is a challenge to create a single interface that meets everyone’s preferences. However, it is a flaw for small organizations that lack the work force, ability, or desire to customize commercial off-the-shelf (COTS) software, thus reducing Remedy’s marketability. One class member suggested that BMC could improve its usability and product acceptance by providing three templates:

* complete (today’s default),
* a more specialized version for help desk and asset management, and
* a single-screen help desk only for small outfits.

An interesting sub-discussion focused on a case where one IT manager disbanded the HD after implementing user-facing HD software. The manager’s expectation was that each user would use the software to report issues. He expected the software’s built-in triage function to route the issues to appropriate support teams. The manager believed that both users and IT staff would monitor system reports to track status. This perception eliminated effective service to those users who could not or would not use the software. This viewpoint also provided no capability for dynamic re-prioritization or a method to correct routing of misreported issues.
MK adds: The case of the disappearing HD should remind readers to _test_ new approaches to operational problems before implementing them in production. The hopeful manager could have avoided some of the problems described above by running a pilot project with a few users instead of replacing the HD outright. Preliminary findings could have prevented the fiasco and prevented a loss of credibility for the team.

In the third and last part of this series, Mani and Rick summarize some interesting issues about triage and politics.

**Mani Akella, CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing Information Assurance and Surveillance services to its clients. He can be reached via email at <mani@consultantgurus.com>. His personal blog is at <http://akellamani.blogspot.com>.

Rick Tuttle is a project manager at Sasol North America Inc., a Houston, TX based chemical manufacturing company. He manages desktop software deployment, including security patches and updates, and supports the company’s business continuity and compliance efforts. Rick can be reached by e-mail at RangerRickT@netscape.net.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. Akella, R. Tuttle & 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.