Service Management Metrics Significant for CSIRTs

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I subscribe to the _Network World_ e-mail newsletter service just as you do. I particularly appreciate the notifications about white papers in relevant areas that I work in for my consulting practice beyond security such as help desk management and data center operations. Today I want to discuss some recent research that bears on computer security incident response team (CSIRT) management.


Why do some organizations manage to run their IT services efficiently and effectively? According to the research published in the ITPI’s study, “Not All IT Controls Are Created Equal: Understanding the performance improvement potential of Foundational Controls,” (available free by registering with the ITPI <http://www.itpi.org/home/white_papers.php>), there were 21 controls in six categories out of a total of 65 controls studied in a survey of 98 North American companies that had “the greatest correlation with the operations, security and audit performance measures. The group’s research shows that the foundational controls were implemented significantly differently in top, medium and low performing IT groups.

In the “resolution controls” category, the four key controls were as follows:

- Track the percentage of incidents that are fixed on the first attempt (first fix rate).
- Use a knowledge database of known errors and problems to resolve incidents.
- Rebuild rather than repair to resolve and incident.
- Have a defined process for managing known errors.

In the Tripwire paper, Mr Kim discusses the following key measures of information technology (IT) team performance:

- Mean time to repair: the best run organizations focus on analyzing what may have changed when problems arise; poorly run groups bumble about rebooting systems without reason.
- First fix rate: good groups fix the problem on their first try in a high percentage of cases.
- Change success rate: how many changes to production systems are implemented without causing disruptions?
- Server-to-system administration ratio: “…high performing IT organizations were not only the most effective, but they were also the most efficient—those with the best Mean Time to Repair, First Fix Rate, and Change Success Rate also had the highest Server to System Administration Ratio.” (p 5)
Chief Information Security Officers (CISOs) will do well to study these reports and think about how to apply the insights to security management. For example, a CSIRT can fruitfully measure how quickly the team analyzes a security incident to find an immediate correction – and also apply the analysis to finding the underlying causes of the vulnerability that has been exploited or the error(s) responsible for security violations.

Similarly, a security team will be concerned with patch implementations as well as planned changes to functionality of production systems, working closely with the programming group and the operations team.

One can predict that, just as in IT operations groups, well-trained and well run security groups will succeed in having a high ratio of servers / systems / users to security officers, thus increasing the return on investment on security equipment, personnel and training.

I think that security is so intertwined with IT that we in the security field can learn much from our colleagues in other branches of the IT field. These research reports are well worth our time and attention.

* * *

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 © 2008 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.