In this continuing series of articles on Computer Incident Response Teams (CIRTs) I am reviewing principles and practical pointers for effective response to security breaches and other operational difficulties in information technology management. Today I’m focusing on some of the advantages, requirements and tools for incident tracking.

_Advantages_

Keeping track of all of technical support calls is essential for effective incident handling. Having details available to all members of the CIRT in real-time and for research and analysis later serves many functions:

* Communication among team members: Having the details written down in one place means that team members can pass a case from one to another and share data efficiently.

* Better client service: Callers become frustrated when they have to repeat the same information to several people in a row; a good incident-tracking system reduces that kind of irritation.

* Documentation for effective problem-solving: A good base of documented experience can help find the right procedure and the right solution quickly.

* Institutional memory: When experience is written down and accessible, the organization’s capacity to respond quickly and correctly to incidents improves over time.

* Follow-up with clients: Managers can use the incident database to prepare management reports and to follow-up with specific clients to understand and resolve difficulties or complaints.

* Forensic evidence: Detailed, accurate and correctly timestamped notes can be a deciding element in successful prosecution of malefactors.

_Requirements_

Some of the more obvious requirements of any incident-handling system are listed below. Most are self-explanatory but I've added comments to a few of them:

* Unique identifier for case
* Dates and times for all events

* Who currently controls the case: It should be instantly obvious who is in charge of solving the problem.

* Keywords

* Contact information: Every person in the case should be listed with room for phone, e-mail and fax numbers.

* Handover of control: Whenever someone takes over control of the case, that handover should be noted in the record.

* Technical details including
  
  o Diagnostics
  
  o Tests of hypotheses

* Resolution: What was the outcome? When was the case closed?

* Search facilities: Full-text search capabilities.

* Knowledge base: Ability to integrate vendor-supplied entries to speed research.

In an online discussion by someone called “DonaldA-M” I noted two additional points I hadn't thought of:

* Industry-standard database engine: Easy to learn, maintain and improve.

* Accept input from comma-separated value (CSV) files: Import data from other systems.

**Tools**

There's a wide range of software available for tracking incidents. You can build your own, but then you'll have to provide proper documentation and training materials because turnover is a constant problem for CIRTs. In addition, unless your analysts have experience with the CIRT function, they are likely to miss useful features that have accumulated over the years in products used by thousands of people.

I have provided a short list of proprietary (commercial) help desk products in the Readings section below. You will want to use the Network World Fusion search at <http://search.nwfusion.com/query.html?qt=help+desk&> to see an extensive list of articles on this topic.

There are also well-respected open-source tools listed below.

All such tools can be complex; since you don't want people fumbling about in an emergency, be
sure that you budget for adequate training for your staff as you implement the tool you select.

***

For Further Reading

“DonaldA-M” (2003). Good, but there’s more… < http://tinyurl.com/4bcve >

Cerberus Helpdesk < http://cerberusweb.com/ >


Help Desk Institute < http://www.thinkhdi.com/ >


Open Source Ticket Request System (OTRS) < http://otrs.org/ >

Request Tracker (RT) < http://www.bestpractical.com/rt/ >

TrackIt! < http://www.itsolutions.intuit.com/Track-It.asp >


***

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business & Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

A Master’s degree in the management of information assurance in 18 months of study online from a real university – see < http://www3.norwich.edu/msia >.

Copyright © 2004 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.