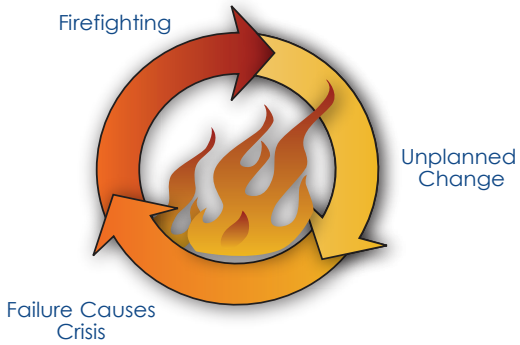
Preventing IT Fires by Managing Change

Change is the root of problems

The story has unfolded in so many ways that nearly everyone has been through some variant. A developer makes a seemingly innocuous change to the Web server, and the IT organization spends the next day trying to figure out why the company's Internet sales suddenly dropped to zero. An employee clicks on a malicious attachment and the company struggles to keep its confidential data from leaking out. A critical server has to be re-hosted and the needed components can't be found — and the administrator who did it last is no longer with the company.

When problems such as these occur, IT organizations have no choice but to go into firefighting mode to make a quick repair. But firefighting itself leads to a vicious circle. Firefighting is, by its very nature, unplanned work. In the rush to fix a critical problem, changes get made that have unintended side effects, sowing the seeds for the next crisis. From this perspective, an organization in firefighting mode actually creates more work for itself, making it even harder to break out of the cycle.

Change is the source of most problems in information technology. Most of the time when a critical problem appears, the root cause is a change in the environment. Sometimes a change causes a problem immediately, making diagnosis straightforward. Other



times a change can cause a problem that doesn't appear for weeks or months, increasing the time to diagnose. When a change is made by someone outside the organization, troubleshooting can take even longer. In any case, most of the time that it takes to implement a repair is spent trying to find the root cause, which is most often the change itself. Wouldn't it make sense to manage change as a planned, less error-prone activity rather than as a reaction to a crisis?

The sign of a mature IT organization

The only way to get out of the vicious cycle is to implement and use change management procedures. Not because it's part of a standard, or because it's required by government regulations, but because it's the right thing to do. Managing change reduces the amount of firefighting that takes place, ultimately helping an IT organization's very mission by raising its quality of service.

Change management is the first step in the quest for the holy grail: Information Technology Infrastructure Library (ITIL), a set of concepts and practices for managing IT services, development, and operations. We all know that we must learn to walk before we can run, and change manage is a lightweight and highly effective step that can dramatically improve the quality of your IT operations. It's like putting oil into your car. It makes it run more smoothly and helps you get where you're going faster.

Change management helps to avoid problems by increasing upfront communication throughout IT and the business, and by identifying and avoiding pitfalls before they happen. Believing in change management means everyone in the IT organization is accountable to surface planned changes before they happen, and to accept feedback from peers with the goal of improving the probability of success for a change.

If a crisis does occur, an organization with effective change management responds differently than one without it. Because change is the cause of most problems, the first response to a crisis should be to review the change logs for the system or application that has failed. Chances are good that the problem can be identified through entries in the change log without even touching the system in question. If the change log doesn't reveal the source of the problem, the next step is to examine the systems on which the one in question depend. Working on the assumption that change causes problems helps to reduce mean time to repair (MTTR), which in turn increases service levels. That's good for everyone.

Rehabilitating your organization

It's exciting to be the cowboy who rides in to save the day. It's difficult to wean an organization off the adrenaline that goes into action when a crisis arises — especially in a culture that often elevates the importance of individuals over what's best for the group as a whole. Here's how you can rehabilitate your organization:

1. Clear the scene. Identify your most fragile systems — the ones causing you the most problems — and eliminate access to

them. Consider limiting access to all of your systems so that only planned, not unplanned, changes are made.

2. Create and document a change policy. This can be as simple as "no changes to this system unless authorized by the employee in charge of it." It is more likely a policy of implementing changes in a planned, documented manner with a review of proposed changes before they are made.

3. Notify stakeholders. Make sure everyone knows and understands the new policy. Everyone must subscribe to it: the IT organization and software developers, managers, and implementers.

4. Create change windows. As your organization comes under more control, negotiate with stakeholders to limit changes to specific change windows. Ultimately you'll want to have a few hours per week during which changes to production systems can occur. This helps to limit the amount of firefighting, and it forces an organization to take time to review changes and plan for implementing them — including a back-out procedure if the change does not go as planned.

5. Reinforce the process. Make change management part of your culture using the carrot and the stick. Reward those who uphold the policy. Catch culprits making unauthorized changes with host-based intrusion-detection software such as ossec or Tripwire.

Implement a change-tracking system

This is the fun part. A ticketing system helps to manage the flow of activities in an IT organization, and it maintains a change log. There are lots of good solutions embodied in both commercial and open source software (see sidebar).

RESOURCES

CA Service Desk Manager *can help with problem tracking and root-cause analysis.*
http://www.ca.com/us/service-desk.aspx

Heat *is a customizable call-logging and tracking system from Targetfour.*
http://www.targetfour.com/hd/products/heat/index.htm

Ionix *is an ITIL-compliant suite from EMC.*
http://www.emc.com/products/family/ionix-family.htm

MantisBT *is a web-based bug-tracking system based on PHP and MYSQL.*
http://www.mantisbt.org/

Remedy Action Request System (ARS), *is a client-server product from BMC Software.*
http://www.bmc.com/products/product-listing/22735072-106757-2391.html

The goal of using a ticketing system is to document changes and automate approval. Decide as part of your policy what level of approval is needed for what kinds of changes. Low-risk changes (such as adding a user) require less approval than high-risk ones (such as applying a patch). Convene a change management team weekly to review proposed changes and assess their potential impact and interaction with other changes.

Change Management at Applied Trust

At Applied Trust, our workflow revolves around our custom-developed ATREK ticketing system. We systematically plan, approve, test, and document changes at a level appropriate with the size, complexity, and sensitivity of the system, whether it is our own or our client's system. Our ticketing system allows us to maintain consistency, and it helps us work as a team.

All production changes are logged with a ticket. Changes to a single workstation or laptop are routine and don't need to be approved beforehand. But if a system is critical, if its failure would affect more than one system, or if it requires coordination with outside parties, a proposed change must flow through our change management process. At Applied Trust, the process includes the following elements:

- An ATREK ticket that is open and kept up to date
- Communication that is early, often, and directed to the appropriate people
- Approval to the level required by Applied Trust (internal changes) or the client (client systems)
- Scheduling to minimize impact and allow time for client and peer review
- Documentation that is thorough, up to date, and easy to find in the ticketing system or an internal wiki
- Monitoring is set up or maintained for services that would affect others if they went down
- Backups of data, applications, and configurations are created and maintained as appropriate
- Security implications of each change are considered and they influence how implementations are done.
- Test and rollback plans provide a way out of the worst-case scenario in which a change goes awry
- High-priority services are monitored and tested before and after a change

Change management is for everyone

Change management is for everyone. It is an essential tool for breaking out of the vicious circle of fighting fires and making unplanned changes that eventually cause more problems.

Fortunately, implementing change management means the addition of some lightweight tools wrapped with a little discipline to use it. Once you've implemented change management, it will improve the way your organization works. ■