Change Control

Louis Aiken

Since authorized changes must occur to networks and these changes must occur in a timely manner without disruption or compromise to existing system operation.

And unauthorized changes must be detected as intrusions or misuse. [1]

Everyone in your organization should understand and abide by the Change Control Policy. Stress the importance of proper use of the policy to all employees. Explain that the policy is in place to help, not hinder operations and the policy is part of the overall corporate strategy. Explain that the policy applies to everyone and is monitored. Insure all employees are aware of the consequences for failing to abide by the policy.

Change Control is the process for the approval, testing, implementation and documentation of changes to your networked devices. It will be part of your Network Policy and will be unique to your operation.

When new features are to be added to any production network the Change Control Policy should always be followed. [4] The following will outline key points.

Is the change needed? What will be the benefit?

A new Network Change Request should be reviewed and approved by a panel representing all departments involved or affected. The panel should consist of experts familiar with all aspects of the enterprise. The panel members should insure their respective departments are able to support the change before approval. Communication is key at this stage. Highly experienced consultants may be needed.

Planning and testing.

Plan, test and document the installation, removal [4], backup, restore, security and upgrade procedures of the system change in a non-production lab environment. Remember that the author of the change stopped testing at some point and "it is impossible to fully test a program"[10] Bugs discovered in the lab environment tend to educate.[8] Bugs discovered after a change has been put into production can have devastating effects on a business. [2] [3]

Documentation.

Clean up the notes from the lab and fill in any holes. Test your documentation.[9]

Implement the change.

When the change is preformed, insure current backups are available and notify everyone that may be impacted by the change. Insure the change performs as expected and has not degraded existing operations. Integrate the change into normal and emergency (if required) operation procedure documentation.

Change Control Policy is good for business. If your company is ISO9000 certified the change control process was reviewed as part of the certification process.[5] Change Control history lays the framework of how your network was built and can be a valuable tool when things go wrong. Insure the history can be made available even if the network is down. This history should be considered confidential but should not contain passwords for the effected component. System passwords should be handled in accordance with the Password Policy section of the Network Policy.

The overview above attempts to outline Change Control in a network administration and security (information assurance) setting. Change Control is often called Configuration Management.

The Change Control Policy for Y2K issues at the National Institutes of Health can be viewed at: http://wwwoirm.nih.gov/y2000/changepolicy.htm [6]

Change Control may exist at different levels within the same company. For instance if your company develops software or documentation, the developers may use change control tracking software as revision control to insure orderly updates, approval and testing of their code.[7] This form of change control might be tied to any product.

[1] Barrus, Joseph and Rowe, Neil C.A
"Distributed Autonomous-Agent Network-Intrusion Detection and Response System"
July 1998
URL: http://www.cs.nps.navy.mil/people/faculty/rowe/barruspap.html
(8-19-2000)

[2] Matt Hamblen. "Software upgrade sparked AT&T outage" 04/22/98
URL: http://www.idgnet.com/crd_at_16074.html
(8-19-2000)

[3] CNNfn, "System failure strikes E*Trade - Feb. 3, 1999" February 3, 1999
URL: http://www.cnnfn.co.uk/1999/02/03/technology/etrade/
(8-23-2000)

[4] University of Kentucky "Standards and Procedures"
URL: http://www.uky.edu/~change/sp.html
(8-23-2000)

[5] ISO9000
URL: http://home.earthlink.net/~reolson/iso9000.html
(8-23-2000)

[6] National Institutes of Health “Change Control Policy” 05/09/2000
URL: http://wwwoirm.nih.gov/y2000/changepolicy.htm
(8-23-2000)

[7] Gary North, "Change Control: Retaining Coherence While Changing the Code" 11-09-1998
URL: http://www.garynorth.com/y2k/detail_.cfm/3042
(8-23-2000)

[8] Network World Fusion News
“How we did it and failure results: InCharge Switch Connectivity Manager failure results”
Copyright 1995-2000 Network World, Inc.
URL: http://www.nwfusion.com/reviews/1025rev2.html

(8-23-2000)

[9] Cem Kaner, “Liability for Defective Documentation” Copyright 1997
URL: http://www.kaner.com/baddocs.htm
(8-24-2000)

[10] Cem Kaner, “The Impossibility of Complete Testing” Copyright 1997
URL: http://www.kaner.com/imposs.htm
98-24-2000)

[11] CNET Networks, “CNET Features - Digital Life – Bugs”
Copyright 1995-2000 CNET Networks, Inc.
URL: http://coverage.cnet.com/Content/Features/Dlife/Bugs/ss05.html
(8-24-2000)