






Identifying Critical Change Control Failure Points

There are key systems in every infrastructure where unapproved change poses significant business risk. The business risk can be outage, integrity of operations, security and audit weaknesses.

What are examples of such systems? The table below shows critical change control failure points identified by companies in various industries: For instance, Los Angeles World Airports (LAX) identified servers housing the database that controls access to various areas of the airport as critical. If unapproved changes were made to these machines, it would compromise the integrity of the airport operations and potentially the safety of passengers. Network Appliance identified their Siebel systems because unapproved changes

created an audit weakness, which could result in restatement of financials. Ericsson identified their ERP systems running on Windows NT as critical because of the fragile nature and high risk of outage. In summary, each of these companies had different business risks, all of which are related to unapproved change.

So how do you identify systems within your infrastructure as key change control failure points? A great starting point is to look at various categories of systems that have characteristics which heighten risk. The following section provides some categorization guidelines that Solidcore customers have used to identify their critical change control failure points.

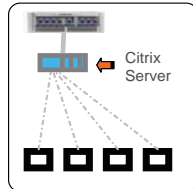
Who	What	Why
	Servers hosting WebEx meetings globally	Critical to customer SLAs
	Transaction processing infrastructure	Critical to maintain integrity of financial transactions
	ERP systems on Windows NT	Fragile systems where any change poses an outage risk
	Physical access control systems	Critical to airport security and passenger security
	Siebel order processing systems	Critical for revenue and to avoid compliance audit weakness

Critical Change Control Failure Points

Systems with Large Fan Out

These are servers on which a lot of machines depend. If they were to go down, a large number of machines would not be able to operate. Examples include:

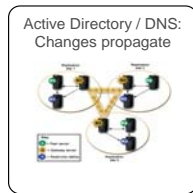
- Root DNS
- Active Directory Servers
- Domain Controllers
- Citrix Presentation Servers
- Virtualized Host Operating Systems



Cascading Changes

A local change propagates automatically through the infrastructure. Examples include:

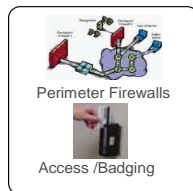
- AD/DNS: Auto-replication propagates mistakes quickly
- Production/Disaster Recovery: auto-sync can bring down both :
- Network: Routing changes propagate quickly;
- Any clustering solution



Access Control Systems

Systems which control access to either the network or the physical facilities including:

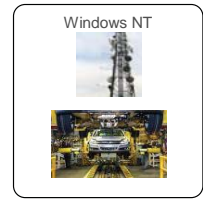
- Checkpoint firewalls on Sun/ Linux Boxes
- ISA/Windows Firewalls
- Physical Access Badging Databases



Legacy Systems

Systems running fragile legacy applications where any change, including OS patches could cause an outage. In use across many enterprises for

- Production control on factory floors
- Legacy ERP systems
- Many other applications



Communication Systems

Communication outages can bring most organizations to a complete halt:

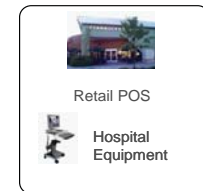
- Email
- Blackberry
- VoIP



Difficult to Service

These machines are difficult to service and cost more to support as a on-site technician is required. In addition people at distributed locations can make often make changes with less scrutiny. Systems include:

- ATMs
- Retail POS
- Medical Imaging Devices



Line of Revenue

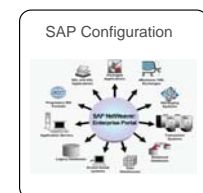
Systems which are in the path of revenue for the company. For example:

- E-commerce
- Order fulfillment etc.
- Servers providing a hosted service for customers



Complex Business Systems

Systems running database based (SAP) or j2ee business applications have complex configurations. Changes to these configurations can cause downtime and bring business to a halt.



Benefits of Categorizing Systems by Business Risk

Categorizing systems according to business risk posed by unapproved change offers several operational benefits:

- The change control board can better prioritize its activities, spending more time on critical systems
- Widely deployed changes can be done in the reverse order of system criticality to minimize risk
- Extra-time can allocated to change windows for critical systems
- Pro-active backups can be performed on critical systems, before changes are implemented

Categorizing systems in this manner also provides a basis for assessing where additional change control measures are required. For critical change control failure points, IT organizations should ask the following questions:

- 1) Do you really know how these systems change? Specifically do you know when changes are made, who makes them, what has been changed and how it was changed?
- 2) Can you easily associate change with authorization? Specifically, do you know that authorized change has been implemented and can you readily identify change that happens without authorization?
- 3) Can you pro-actively ensure that unapproved change doesn't happen?

If the answer to any of these questions is 'no', you may want to look for a change control solutions such as Solidcore S3 Control™, which is specifically designed to provide the high level of change control required for critical systems.

In summary, all companies, regardless of industry, have IT systems whose availability and integrity are critical to the viability of their business. Identifying critical change control failure points in your infrastructure, understanding your current level of control, and adding additional control where needed can eliminate significant risk to the business.

About Solidcore Systems

Solidcore is a leading provider of change control for critical systems. Solidcore's S3 Control software is the industry's first and only solution to automate the enforcement of change management policies. Solidcore automatically reconciles infrastructure changes against change tickets, and provides real-time change auditing so enterprises can measure the effectiveness of change management processes and policies. Customers trust Solidcore to improve service availability, implement ITIL initiatives, and lower costs related to Sarbanes-Oxley compliance.

Solidcore also provides change control for embedded systems and is used by major device manufacturers to securely leverage open systems to meet their business requirements.

Solidcore is headquartered in Cupertino, California. For more information, visit www.solidcore.com

solidcore®

Solidcore Systems, Inc.
20863 Stevens Creek Blvd, Suite 300
Cupertino, CA 95014

Email: sales@solidcore.com
Web: <http://www.solidcore.com>
Tel: 888.210.6530