# Global Information Assurance Certification Paper

Denis R. Lynch
Version 1.2e

**Enhanced Security during Organizational Transitions**

***Purpose***

The purpose of this paper is to provoke discussion concerning the requirements for increased security during a period of transition within an organization. The discussion should revolve around the threats faced by an organization as it goes through a period of change, as well as the controls that exist to mitigate risks.

***Scope***

This document applies to any organization that is undergoing a significant change. This change can apply to employee turnover, layoffs, or a change in organizational structure due to a merger or acquisiton. The document can be used by both public and private sector organizations, of varying sizes.

***Background***

The transition of operations within in an organization can pose serious risks to their ability to perform mission-critical functions. When this transition incorporates the termination or layoff of a significant number of staff members, the risk to the security of organizational information resources is multiplied. As an organization considers a transition within their network operations and infrastructure support, several factors must be considered to minimize the risk to the organization's day-to-day operations. Implementation of appropriate security controls in an expeditious manner will help the organization maintain operations in a seamless manner.

This document describes not only the possible threats faced by management as they proceed with the transition process, but also provides a subset of appropriate controls that could be implemented to mitigate the risks.

***Threat Sources***

The past ten years has welcomed great changes within the corporate world. A glut of mergers, acquisitions, and outsourcing has led to an increased focus on organizational transformation. Throughout the course of these changes, personnel and the information technology architecture will need to be flexible enough to change with the organization. Organizations in transition face threats from all sides—internal, external, external sources colluding with insiders, etc. While it is true that external threats such as hackers and crackers pose a tremendous threat to the security of an organization's information resources, during organizational transition, it is much more likely that the attack will generate from an insider.

The threat to information resources is heightened when the change is impacting the information technology specialists and network support staff within the organization. These employees will possess both the motivation and the means to wreak havoc with the information technology architecture of the organization. Not only do these employees possess the knowledge of how to operate the systems, but they also will have knowledge of any outstanding vulnerabilities that reside on the system or network. These vulnerabilities can be exploited either immediately, or at some point in the future, to take control or disrupt system services.

***Threat Analysis***

As mentioned above, the transition of operations from one organization to another can create additional threats for an organization. If vulnerabilities are exploited as a result of these threats, the organization is placed at an increased risk for degradation or disruption of services. The additional threats faced by the organization during this transition period, along with a brief description of the threats, are listed below.

*Theft:* Theft of both information and physical equipment can have a serious impact on the organization during the transition period. The removal of company-owned data, information, software or hardware could impact the organization's ability to accomplish its mission and business objectives.

*Malicious Code:* Outgoing information technology support staff have the capability, as well as the time and resources, to embed malicious code on systems and applications. Trojan horses and logic bombs can be introduced to activate at dates well after the transition has taken place to relieve suspicion. Also, viruses can be introduced to the networks to seriously degrade and even destroy proprietary information.

*Back Door Access:* Upon receiving notification of the transition, it is possible for the system administrators and affected staff to develop "back doors," which will allow them to gain access to internal networks from outside the organization. These back doors can be used to extract information, introduce malicious code, or engage in corporate espionage.

*Destruction of Equipment and Information:* The physical destruction of equipment and information is possible once the notification of a termination of services has been issued. Physically destroying hardware or software could have serious financial impacts on the organization. In addition, the destruction of data and information could result in a disruption or halt of business processes, seriously impacting the organization's ability to perform its mission.

*Loss of Knowledge:* Although often overlooked, the job-specific knowledge of outgoing staff should be captured prior to their departure. Many times, job-specific responsibilities and knowledge are not documented prior to termination of duties, and valuable time and resources must be expended to recapture this knowledge or re-train existing staff.

*Legal Issues:* HR and management must be aware of all possible legal issues that could arise as a

result of the transition. Wrongful termination suits could be filed; Proprietary information could be removed from the premises. These and many other potential legal issues should be addressed prior to the beginning of the transition.

***Potential Results***

The potential for sustaining heavy damage as a result of vulnerabilities exploited during organization change is high. Loss of data, disruption/denial of service, loss of customer confidence are all very real outcomes for an organization in transition. Without a well-organized and implemented plan for addressing the risks highlighted above, few organizations will be able to maintain their service at a high level. The paragraphs below provide a sampling of security controls that may be implemented to increase the likelihood that a security incident will occur.

***Mitigating the Risk***

The organization will need to address these issues, as well as any others that may arise, while still performing their daily business functions. Preparation prior to the transition will enable the transition process to proceed smoothly, with minimal impact on remaining staff. In preparation for a seamless transition, it is important that the organization's transition team receive complete support from management in implementing threat mitigation measures. This requires keeping management informed of all details, and ensuring rapid notification of changes in strategy and implementation. In addition, several key measures for mitigating the risks posed by the threats above are outlined below.

*Personnel Security:*

- Ensure comprehensive background checks are performed on all employees and contractor staff requiring access to sensitive information and equipment
- Require all employees to sign non-disclosure agreements prior to gaining access to the information resources. It will be necessary to remind the employee of this agreement during the exit interview process.
- Document a "Rules of Behavior" policy for general system users and require a signed letter of acknowledgement stating that they understand, and will adhere to, the rules.

*Physical Security Controls:*

- Change the key and cipher locks at all entrances to critical equipment
- Reprogram swipe card access to the server room.
- Require all employees, regardless of position or authority, to display a badge at all times. All departing staff should be required to relinquish their access badges and keys immediately.
- Increase patrols by personnel security staff, especially during non-business hours. If necessary, have personnel security accompany HR staff to collect badges and office keys.
- All visitors should be signed into the facility and be required to display a badge at all times. If access to sensitive information is required, the visitor should be required to have an authorized employee present at all times.

*Logical Access Control:*

- Immediately log off and disable staff accounts upon termination.
- Require all remaining employees to change their passwords immediately.
- Disable all remote access accounts granted to departing staff.
- Change all administrator-level passwords on existing networks and servers.
- Determine the proper access rights and privileges to be assigned to new/transitioning employees. These rights and privileges should be reviewed on a regular basis to ensure that employees do not "collect" permissions and privileges, granting them access to systems and information that they might not otherwise be authorized to access.

*Network Monitoring:*

- Conduct bi-weekly vulnerability analyses and compare to previous results to determine whether additional vulnerabilities have been introduced by departing employees.
- Increase network monitoring/auditing to identify unusual activity, which could signal malicious activity.
- Audit log files regularly to detect unusual server activity.
- Initiate vulnerability analyses on the networks to identify security holes or back doors that could be used by people external to the organization to gain access to their networks. This vulnerability testing should also include limited penetration testing to determine the extent to which intruders could access information from outside the organization.

*Alerts and Warning:*

- Re-configure the intrusion detection system to notify information security staff when attempts are made to access the accounts of terminated staff.
- Update anti-virus software and run regular scans to check for viruses introduced into the network.
- The organization's incident response plan should be reviewed and tested. Employees should be aware of the procedures for identifying and reporting potential security incidents to management and security personnel.

*Policy and Procedural Documentation:*

- Update/implement all termination policies and procedures – ensure that appropriate staff is aware of these policies and procedures.
- Ensure that the transition process is incorporated into a Business Continuity and Contingency Plan.
- Develop signed agreement stating that departing staff will not introduce threats (i.e. back doors, Trojan horses, malicious code, etc.) into the network prior to departure.

*Inventory*:

- Develop a list of all possible accounts where passwords and privileges need to be revoked.
- Conduct an inventory of software and hardware (barcodes??) to ensure that departing employees do not remove physical plant and equipment. This inventory should be done during non-business hours to reduce the impact on daily operations. In addition, this inventory can be used to identify cost-cutting measures by pinpointing redundant systems and excess waste.

*Data Backup and Integrity:*

- Verify that adequate backups exist to restore the system from a particular date
- Ensure that backup and restore functions are working properly prior to termination
- Conduct regular backups and test these backups for data integrity
- Provide IT staff with policy and procedures to conduct these backups and introduce the backups into the system when necessary.

The implementation of these controls, coupled with the diligence of responsible employees should ensure a seamless transition of network operations and infrastructure support across the organization.

***Conclusion***

As recent events have shown, unexpected events can be devastating to the viability of an organization. Whether the result of a merger, acquisition, or layoff of employees, an organization in transition faces increased risk from both internal and external sources. Organizations may face disruption of service or information loss from both intentional and unintentional events. Intentional events, those events initiated by hackers, crackers, insiders, former employees include introduction of malicious code, destruction of property, theft, espionage, and loss of data integrity. Unintentional events can include data corruption, service disruption, incompatibility of systems, and employee turnover. Whatever the cause, any event that compromises the confidentiality, integrity, and availability of an organization's information resources can lead to significant financial and knowledge loss.

In my opinion, the key to a successful organizational transition lies in the hands of senior management. From the start, management must implement policies and procedures as standard practice across the organization. Strong policy and procedures should provide the foundation for a well-informed organization. Once a decision to change has been made, management should coordinate with security staff to identify necessary procedures and controls that must be implemented to ensure a smooth transition. As these procedures and controls are put into place, it is the responsibility of the security staff to communicate to management any issues that must be resolved, along with potential solutions. Finally, open and honest communication concerning the transition is key. If affected staff feel as though management has been open and honest with them throughout the entire process, especially if management has expended effort to make the transition easy for all parties, the likelihood of a security compromise will be lessened.

While all of the controls mentioned above will not guarantee the security of information resources during a major organizational transition, security should be greatly enhanced by implementing appropriate measures. Awareness is key. If management and security staff are aware of the controls and policies being implemented to safeguard assets, they will be more likely to notice anomalies in data and system integrity. As overall organizational awareness is raised, it will make it increasingly difficult for attacks originating from inside **or** outside the organization to succeed.

## References


Cohen, Fred. "Managing Network Security: The New Cyber Gang -- A Real Threat Profile," Fred Cohen and Associates, 2001 (available at http://all.net/journal/netsec/2001-05.html)

Randall K. Nichols, Daniel J. Ryan, and Julie J. Ryan, *Defending your Digital Assets Against Hackers, Crackers, and Spies*, McGraw Hill Professional Book Group, December 1999.

"The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment," National Security Information Exchange, June 18, 1998.
(available at http://www.ncs.gov/n5_hp/Customer_Service/Aftansie98.html)

"Networked Information Systems: Protecting Against the Threat 2000" available at http://www.nacic.gov/pubs/nis.htm

Krimkowitz, Harry. "Mitigating Risks to the Insider Threat within your Organization," Information Security Reading Room, SANS Institute, October 24, 2000. Available at http://www.sans.org/infosecFAQ/securitybasics/insider_threat.htm