

Ensuring Data Security during Downsizing

Prepared by:
Lowell Smith
Manager
Technology Risk Management Services
RSM McGladrey, Inc.
lowell.smith@rsmi.com
847.413.6950

What makes an economic downturn different than other threats to an organization's success? The key differences are that the impact will be longer than most other threats and that the recovery will be more dependent on external factors, such as consumer confidence, global economic stability and the viability of clients. The length and severity of the downturn can severely impact the demand for products and services, leading to major revenue declines for all organizations.

In light of this external focus, many internal functions of an organization are often ignored. One of the more important activities, ensuring the integrity of data resources, may become lost in the turmoil.

A common response to business shortfall is downsizing staff. If this happens in the technical support area, technical management must be prepared to provide the same level and scope of business support with fewer resources. Finding ways to manage the technical infrastructure to optimize the efforts of the remaining support staff becomes necessary. Of the many support functions provided by technical teams, a key goal must be to continually and properly secure data and infrastructure resources. By maintaining this security for the duration of the downturn, a viable technical platform is available for an organization to land on when the economy rebounds.

We will concentrate on the data security and integrity issues that occur as a result of a reduction in force. Specific risks and control activities are described. Many of these risks and controls are familiar to technical management during periods of normal business activity. However, in a downsizing environment, these specific risks are magnified and controls must be effectively executed to ensure data is properly protected.

The risks

Downsizing during an economic downturn could result in:

- Fewer personnel available to protect information resources, maintain security controls and monitor critical systems
- Fewer development and testing staff available (with the pace of development normally not reduced, the resulting applications may be more error prone and less capable of meeting user requirements, which negatively affects data confidentiality and integrity)
- Reduction of operational and business staff (this reduces time for quality assurance procedures for reports and databases and thereby compromises data integrity)
- Possible segregation of duties issues through merging of roles and assignment of single members of staff to

several roles, allowing a single user to defraud the organization

- Increased possibility of actions by disgruntled or former employees
- Greater possibility of an increase in crime (most importantly cyber crime) due to personal economic crises
- Loss of vendor support from those who are unable to withstand the economic slowdown
- Increase in data and information systems vulnerabilities as a result of all other risks mentioned here

Risks pose a threat to many functions and assets, including data resources. Consider the following major technical resources at greatest risk and what that means:

- Proprietary applications or infrastructure becoming unreliable due to inadequate testing and developers making unauthorized changes in production or the theft and sale to business competitors
- Protection of intellectual property lost through inadequate access control to core servers, resulting in the theft of unsecured trade secrets
- Physical hardware and software lost due to theft or piracy (private and personal ID data on stolen portable computers could become public)
- Vendor-supported infrastructure not kept current due to vendor staff reduction or an organization's efforts to reduce support costs
- Client contact information becoming compromised through unintentional errors or intentional destruction when proper access controls are no longer maintained and enforced or through the theft of improperly secured databases and the sale to business competitors
- Firewalls and Web server security layers not kept up to date, causing an organization Web site and Internet business to become severely compromised by threats such as denial of service attacks
- Compromises to server access that can lead to the corruption of key databases through backdoor attacks or by simple mistakes made by untrained staff reassigned to key data maintenance tasks
- Termination information not quickly communicated to technical support staff due to poor training or overloading of human resources staff members, causing access to not be removed quickly enough (for example, if e-mail access remains enabled, disgruntled employees could send damaging e-mails from the organization's e-mail server)

Addressing risks related to downsizing

A proactive approach is needed to protect an organization from these serious risks. In times of uncertainty and disruption, successful companies present an image of confidence and control and reassure customers and stakeholders that the organization has properly prepared for downsizing and has a plan for the sustainability of business.

When reviewing current vulnerabilities and implementing security solutions, address these eight areas:

Logical security of in-house network and information security systems. Logical security is central to any information security plan; the first and often the second and third lines of defense for technical infrastructure rely on it. The first challenge is network authentication. The second challenge is server authentication and the third is application or database-level access control. If access to organizational resources is immediately removed at the time downsizing actions occur, the temptation for abuse by individuals being let go is removed.

For internal users, client users and business partners, primary logical security is an interactive authentication system, i.e., most commonly a user ID and a password challenge. Passkeys and confidential security questions may also be used. The most significant password management issue is to notify security administrators of all terminated individuals for immediate removal from local and remote access methods.

Secondly, password parameters and password administration, e.g., password complexity and length, expiration period and limiting use of previous passwords should be made as strong as possible. Password authentication and user profile restrictions can be enforced at the network, server, application and database levels.

Terminated users, if disgruntled, can become an external threat. With unauthorized remote access, the user may use hacking, denial of service, hijacking and spoofing methods to attack the network. To reduce this risk, present interfaces to the outside world that are as secure (hardened) as possible.

Evaluate and further strengthen these security solutions by utilizing:

- Firewalls and routers
- Data transmission tunneling and encryption
- VPN solutions for working remotely
- Antiviral software for all servers and user systems
- Hardening of outward-facing servers by restriction of available ports and services

Administration of these logical security controls must continue during and after downsizing. When controls are properly designed and enforcement procedures are implemented, the effects of downsizing are minimized. Review staffing assignments to ensure sufficient administrative coverage continues and make sure staff is trained to enable, disable and monitor access to all critical systems.

Physical security of the environment surrounding technology infrastructure. As an additional first line of defense, closely review security measures of the facilities that house technical resources and business locations that house users. Reviews of current holders of keys and keycards, visitor policies and an evaluation and strengthening of procedures to retrieve keys from departing staff members must be undertaken.

Data integrity and confidentiality. Attacks and errors, either intentional or accidental, may destroy or corrupt critical client and organization resources. A key risk in downsizing is losing knowledge of data integrity procedures and checks.

Undertake these activities to address threats to data integrity and confidentiality:

- Update documentation of operational procedures.
- Adopt enhanced encryption methods and procedures during data transmission and for data at rest, as well as require similar commitments from business partners.
- Reinforce, limit access to and further automate data transmission procedures.
- Partition data storage where user access is restricted on a need-to-know basis.
- Add data validation procedures to ensure data is not manipulated during processing.
- Limit administrative access to systems and data as much as possible and log all activities for critical systems, ensuring that logs are reviewed for any suspicious activity.
- Develop recovery programs for all critical data that provide rollback capabilities to meet business needs.

Segregation of Duties. Downsizing poses a problem for upper management and departmental structures that help ensure proper checks and balances are in place to address fraud and collusion. Downsizing decisions should be predicated to ensure segregation of duties is not compromised. Work efforts must continue to be understood and carefully monitored and after the reassignment of responsibilities, checks and balances must remain.

Tools to help in this process include:

- Current process flows including roles and responsibilities
- Updated segregation of duties matrices for all critical business and support functions (management meets prior to downsizing to reassign roles and tasks and then reviews revised matrices for any conflict of duties)
- Mitigating manual and system controls to provide improved management oversight of activities

Monitoring of activity. Often downsizing includes a significant reduction in management at various levels. If departing managers had significant roles in the oversight of operational, business and financial processes, the risk of losing supervisory control is high. Supervisory control is often a mitigating control and, if lost, primary controls may need to be reinforced by remediation to properly address the risk. If downsizing affects the network administration staff, the monitoring of network and systems access and usage could suffer.

Monitoring internal users is important to ensure they are not accessing resources they are not authorized to access. Similarly, monitoring client usage helps verify that client users are only accessing their data, not other client data or internal network resources. The primary value of monitoring is detecting suspicious activity from unusual sources or from users no longer authorized for access, including departed employees.

To address the risk of inadequate manual monitoring and oversight, review and strengthen the following automated controls where possible:

- Enhance electronic network monitoring with management alerts activated.
- Activate database logging and implement alerts for excessive activity.
- Develop electronic dashboards with alerts and install on management desktops so that monitoring can proceed with greater efficiency and less direct contact.
- In addition, logical access solutions already discussed can serve as preventative controls against unauthorized access.

Change management. Risks to change management include the loss of staff to the degree that independence of development, testing, acceptance and implementation is compromised. This can lead to segregation of duties issues between development, testing and installation functions of software and can degrade the integrity of resulting software. If the software is compromised, an organization is subject to a plethora of risks, including data manipulation, trojan/backdoor software, key loggers, logic bombs, data integrity, data confidentiality, business continuity, loss of intellectual property, fraud and potential extortion.

Consider these software development life cycle adjustments:

- Extend development periods.
- Reassign roles to remaining staff that have the necessary skills.
- Outsource the entire development cycle or offshore portions of the development cycle such as testing. One cautionary note about outsourcing: it cannot be delegated and then ignored. The software owner is ultimately responsible for the functionality and integrity of the end product and several organizations have found offshoring takes significantly more effort than expected to ensure the product met an organization's standards.

Vendor and patch management. Maintaining hardware and software can be more difficult in a downsized environment. Security patch frequency may actually increase due to more desperate hacking activity. An organization may experience decreasing support from vendors who have downsized themselves. Select secondary vendors for all critical technical resources so that support can continue if the primary vendor is unable to provide adequate support.

There are several money-saving steps, including reducing seat license levels in software contracts and negotiating service contracts more vigorously to receive reduced rates from vendors that do not want to completely lose your business. Economic pullbacks can be an ideal time to upgrade hardware at much reduced costs with the added advantage of newer technology providing greater efficiency and security with less effort.

If costs need to be reduced further, evaluate the possibility of pursuing vendor support of servers to replace in-house system administrators, but ensure that vendor access is restricted as much as possible. Take advantage of automated options for installing patches, as well as updates in firewalls and antivirus software to reduce manual tasks. Consider purchasing firewall appliances that have automated update features to reduce maintenance overhead.

Training and documentation. The departure of knowledgeable staff may expose a very significant deficiency in management activities. It may become obvious how little documentation of key business and operational processes exist and that an organization has functioned largely on the memory of a few long-term employees.

Prior to downsizing activities, gather and evaluate all existing documentation. Where it exists, update usable documentation to represent current requirements, procedures and dependencies. Close all remaining documentation gaps with a concerted effort to

describe all critical business and operational functions including inputs, outputs, dependencies and verification mechanisms. Identify critical functions through an analysis of the value provided and the criticality of other procedures dependent on it. As documentation is created, organize training sessions to inform all responsible staff and walk through the procedures described. Walk-throughs serve to improve documentation, but also to uncover possible enhancements to procedures that may improve efficiency and security.

Conclusion

The current economic conditions are posing a number of problems for all businesses. Downsizing is an option that several companies are turning to, which in turn, could compromise the security of your data. Following the steps presented here could go a long way to ensure that your company is better protected against the growing number of threats and vulnerabilities in your information systems.

To learn more about RSM McGladrey's services, call 800.648.4030, e-mail us at TRMS@rsmi.com or visit us online at www.rsmmcgladrey.com.

RSM McGladrey, Inc. and McGladrey & Pullen LLP have an alternative practice structure. Though separate and independent legal entities, the two firms work together to serve clients' business needs. RSM McGladrey, Inc. is not a licensed CPA firm.

RSM McGladrey and McGladrey & Pullen serve clients' global business needs through their membership in RSM International, the seventh-largest worldwide organization of independent accounting and consulting firms (source: *International Accounting Bulletin*), with 680 offices and 27,000 professionals in 65 countries.

To learn more, call 800.274.3978 or visit www.rsmmcgladrey.com.

RSM! McGladrey
Accounting | Tax | Business Consulting