

Managing IT Risks During Cost-Cutting Periods

Mark Nicolett, Paul E. Proctor, French Caldwell

To provide visibility into increased risks that can result from crisis-driven budget cuts, risk assessment should be a prerequisite to proactive IT cost cutting. The world financial crisis of 2008 will drive proactive cost cutting in very short time frames, but cost-cutting risk is better controlled when staff and projects are aligned with service delivery, new capabilities and line-of-business budgets.

Key Findings

- Risk management, compliance and security professionals can support IT organization and business cost-cutting initiatives by providing IT risk assessment support, ensuring that reductions in security budgets are appropriate and minimize risk-posture impacts.
- The evaluation of sourcing alternatives for IT functions should include service, security and compliance requirements.
- Security staffing decisions should ensure that basic security capabilities and required project support are maintained.

Recommendations

IT risk managers should:

- Work closely with IT financial managers and business analysts to initiate cost-cutting risk analysis before senior management imposes cost-cutting mandates.
- Support the decision-making process with good business and IT risk intelligence so that cost-cutting actions do not expose the organization to unacceptable risk levels.

Compliance managers should:

- Confirm that proposed cost cuts do not impact regulatory, commercial or organizational mandates.
- Ensure that appropriate governance procedures are followed regarding input rights and decision rights regarding cost cutting.

Security managers should:

- Define and document current security operations and identity administration service levels to assess cost-saving opportunities and the budget and service risks that are inherent in sourcing decisions.

- Allocate the staff to security operation tasks that are needed to provide basic services, and project work to improve infrastructure protection and for secure business enablement.

ANALYSIS

Ignoring or misunderstanding financial risks played a substantial role in creating the world financial crisis in 2008. Gartner expects cost-cutting mandates as the downstream effects of the credit crunch begin to affect many businesses (see "Economic Downturn: Beware the 'We Aren't Seeing It' Trap"). Organizations need to assess risk as part of cost-cutting decisions and should manage increased IT risks to prevent operation failures that will lead to further loss.

In many cases, cost-cutting mandates will be expressed in relatively simple terms, such as reducing budgets by a specific percentage in a relatively short time period. These cuts will be implemented through staff reductions, technology consolidation, postponement or elimination of discretionary projects and sourcing changes. This inevitably will lead to direct and indirect controls that will increase service, security, compliance and capability risks. At the same time, IT risk management and security professionals will be challenged to make cuts that directly affect infrastructure protection, identity administration and other security, risk management and compliance services related to the business (see "Cost Cutting While Improving Security"). Careful attention to the risks these cuts can impose on IT services can prevent unexpected, negative effects on the business' goals and objectives

Fundamental Gartner guidance for this difficult time includes:

- Create a cost-cutting team.
- Focus on people.
- Get creative in your approach to cutting costs (see "Time to Get Creative: Business as Usual Doesn't Cut It").

Risk management, compliance and security professionals should participate in the cost-cutting process to assess IT risk and enable good decisions that do not leave the enterprise open to unacceptable risk levels. The group that owns the risk is the business, not the IT organization or the risk management and security teams. If cost-cutting decisions are made that significantly impact the risk posture, then the business should be apprised of the change and be given the opportunity to object. The business should also sign off on the final plan with a nontechnical statement of the new risk posture. This is done more easily in an organization that has a mature risk governance process.

IT risk management, compliance and security professionals must support cost-cutting exercises by providing IT risk assessment support and managing appropriate reductions in IT risk management and security budgets, while minimizing risk posture impacts.

Risk Assessment Support for IT Cost Cutting

Across a typical company, cost-cutting strategies can include external sourcing, centralization of departmentally managed IT resources, staff reductions, alternative delivery models, such as software as a service (SaaS), and the use of consumer-grade applications, among others. Each of these cost reduction actions requires a risk assessment, and some of these actions will require additional project work and ongoing support resources from IT risk management, IT security and IT operations.

- **Infrastructure centralization, consolidation and unification:** Cost reduction is achieved by centralizing IT that is currently owned and operated by the business units or departments. To ensure that risks are properly identified and managed, risk managers should work closely with project managers to conduct project risk assessments and risk

reviews at each major milestone. They should also work with IT financial managers to ensure that project portfolio management includes good quantitative risk analysis. Security operation teams must support project work to incorporate the infrastructure into centralized security administration processes and infrastructure protection technologies. Longer-term project work also will bring systems into standards compliance.

- **External sourcing:** Outsourcing is frequently evaluated as a means to reduce IT labor and technology investment costs, and organizations may also evaluate new cloud-based offerings. The evaluation of potential service providers must include an assessment of security and privacy controls, which will require the resources from the security and risk groups. Ensure that service provider assessment methods are well-defined, that business areas understand the need for a risk assessment and that the assessment is done before the sourcing decision is made (see "Gartner Survey Highlights Company Burden of Vetting Third-Party Security Controls" and "Assessing the Security Risks of Cloud Computing").
- **SaaS:** SaaS solutions have the advantages of lower upfront costs than an on-site application license, and less involvement is needed from the IT organization. Enterprises that may have rejected a SaaS solution in better economic times for security or architectural reasons might shelve those concerns when finances get tighter. Although SaaS is a viable alternative, it is important to mitigate the risks by doing a good security review of the solution, and assessing other vendor risks, such as viability and management operations. Additionally, the enterprise must be cognizant of preservation obligations, which cannot be shifted to a third party. Furthermore, if integrating a SaaS solution with other applications, then an architectural review to determine compatibility with enterprise architecture is important. A SAS 70 audit report from the vendor is not adequate assurance that the solution will meet all of an enterprise's risk mitigation and control requirements (see "How to Manage Risk in Alternative Delivery Models" and "Critical Security Questions to Ask a SaaS Provider").
- **Consumer-grade IT:** There may be pressure to avoid software and hardware procurement costs by using consumer-grade applications, and by encouraging employee PC purchases and self-support. A risk assessment is needed to identify low-risk user populations for employee-owned IT technology. Compensating controls, such as network access control and data loss prevention, may need to be evaluated. For consumer-grade applications, the IT security organization will need to work with the business areas to define appropriate use cases and constraints, and will need to educate business areas to minimize compliance and data risk (see "Optimal Security Approaches for the Secure Use of Consumer IT").

Risk managers should be aware that the interactions among various cost-cutting actions could create unforeseen risks, and they should strive to identify the interactions among cost-cutting actions. For instance, a move to consumer-grade IT may be manageable when the enterprise manages its own infrastructure. However, what will happen when the infrastructure is outsourced as an infrastructure utility?

Cost Cuts in the Security Organization

Like any other area in the company, the IT security organization may need to respond to a request for budget cuts. The preparation for this request is similar to work done in other areas — that is, define the services currently provided, allocate staffing resources to core infrastructure protection functions and identity administration functions, current compliance initiatives and future project work (see "Making Do With Less: Tactics for Managing the Impact of Security Budget Cuts").

- **Staffing and outsourcing:** IT security staffing levels are typically low and do not provide a large cost-cutting opportunity. In larger organizations, however, there may be opportunities to reduce security operations center (SOC) staffing by using network security operations for first-level monitoring, or by outsourcing SOC functions to a managed security service provider.
- **Endpoint protection:** A large percentage of the security budget is expended on endpoint protection. Opportunities may exist to reduce costs at the time of endpoint protection software license renewal (see "Cost Cutting Endpoint Protection Platforms" and "Q&A for How to Improve Mobile Security on a Stationary Budget").
- **Identity and access management (IAM):** IAM projects that were planned to support new outward-facing applications should be delayed if the application deployments are postponed to reduce costs. Staff reductions in other areas will require decommissioning access rights for users who are no longer with the enterprise. Outsourcing in other areas requires changes to user provisioning processes (see "Cost Cutting in Enterprises, and Six Ways Identity and Access Management Programs Can Help").

The IT organization, IT risk managers and the lines of business need to be aligned regarding the risks associated with cost cutting. Cost cutting will probably amount to a reduction not only in service levels, but also in control of confidentiality, integrity and availability. The participating organizations and managers need to first recognize that risk is increasing, and then agree that an increase in risk is needed to achieve short-term cost-cutting goals. Business managers must acknowledge that risk tolerance is being increased, which may require more management attention to monitoring risk. The security bar may have to be lowered, and managers will have to agree that this and other actions are acceptable temporary compromises.

Time for Strategy

Gartner predicts that there will be increasing regulations as a result of the 2008 financial crisis. Therefore, this is no time to ignore risk management and compliance. Furthermore, economic uncertainty means that decision making becomes more risk-adverse. Without good risk intelligence, decision makers could overreact and limit enterprise agility, or they could miss risks that could undermine business goals and objectives.

Risk management and security professionals should use this opportunity to act strategically, become more risk-aware and achieve greater resilience (see "IT Innovation Will Be Key to Turn Economic Crisis Into Opportunity"). A process-driven approach to security and risk management will improve efficiency, transparency and measurability, while improving the enterprise's risk strategy. Organizing the management, measurement and reporting of controls through good IT governance, risk and compliance will support an organization's overall maturity.

RECOMMENDED READING

"Cost Cutting While Improving Security"

"Making Do With Less: Tactics for Managing the Impact of Security Budget Cuts"

"Cost Cutting Endpoint Protection Platforms"

"Cost Cutting in Enterprises, and Six Ways Identity and Access Management Programs Can Help"

"Q&A for How to Improve Mobile Security on a Stationary Budget"

"Optimal Security Approaches for the Secure Use of Consumer IT"

"How to Manage Risk in Alternative Delivery Models"

"Critical Security Questions to Ask a SaaS Provider"

"Gartner Survey Highlights Company Burden of Vetting Third-Party Security Controls"

"Assessing the Security Risks of Cloud Computing"

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509