Gartner Research

Publication Date: 27 May 2009 ID Number: G00167541

Four Risk Management Mistakes That Threaten Your Security Budget

Jay Heiser

Enterprise security budgets have always been difficult to justify, and the global economic crisis is making this critical process even more difficult. Use this guidance to align your security and risk practices with business objectives — and to protect your security spending.

Key Findings

- Security efforts are most likely to be inappropriately low when business decision makers fail to recognize the value of security and its impact on their business goals.
- Enterprises that develop relatively mature information security programs typically spend less on explicit security costs than comparable organizations do.
- Most CIOs and chief information security officers (CISOs) have allowed themselves to assume accountability for risk that should be "owned" by the for-profit lines of business (LOBs).
- The IT organization and IT security must meet specific business needs for risk control. Security service-level agreements (SLAs) that make risks and risk controls explicit are practical mechanisms for achieving this goal.

Recommendations

- Align IT security and risk management practices and controls as closely as possible with the needs of the business.
- Help LOB managers to understand and accept accountability for risk that potentially affects the IT systems, information assets and business processes that they "own."
- Develop a simple, typically three-level system for expressing the business-criticality of specific data, information, and processes, and enforce its use enterprisewide to establish security SLAs.

WHAT YOU NEED TO KNOW

The keys to justifying and optimizing security spending are to ensure that security and risk control practices are meeting explicit business objectives, and — crucially — to persuade the business to take ownership of risk. Security professionals are unlikely to achieve these critical goals if they fall into one of these four common risk management mistakes.

ANALYSIS

Enterprise IT security professionals face a complex, even paradoxical situation as the worldwide economic crisis continues. In a period of highly constrained financial and staffing resources, they must manage and mitigate a rapidly changing and expanding risk environment. They must respond to expanding regulatory and other legally relevant requirements. Most enterprise IT expenditures are inevitably coming under intense scrutiny during this period of economic difficulty, and IT security and risk management spending — although less-radically affected than overall IT budgets — is no exception (see "2009 Update: What Organizations Are Spending on IT Security").

The coming year will unquestionably be a period of extreme uncertainty, and most enterprises and internal organizations will be forced, at a minimum, to contract their planning time horizons, thereby focusing on short-term issues and postponing some long-term plans. Many Gartner clients have reported, however, that their IT risk budgets remained strong through late 2008 and the first quarter of 2009. We see two fundamental reasons for this:

- Enterprises' recognition that IT risk is increasing, not declining
- Pressure for improved governance from governments and regulatory bodies worldwide

Nonetheless, IT security and risk professionals mustn't make the mistake of assuming that their budgets aren't threatened — because they are.

CIOs, CISOs and other IT security professionals have always struggled to make the case for security spending. This isn't surprising because most enterprises' information security planning processes are fundamentally flawed. They fail to align IT security and risk practices with the priorities of the business, and, most crucially, they don't make the business take explicit responsibility for IT risk (see "No More Dr. No: Developing a Strategy for Business-Aligned Information Security").

IT risk — the need to assess it, manage it, mitigate it, and, when necessary, accept it — is the reason why the information security organization exists. However, this doesn't mean that the IT security group, or the larger IT organization, should allow itself to "own" risk. The proper place for that accountability is with the business — with the senior executives and LOB managers whose budget supports the IT systems and information assets that you're trying to protect. Providing security services is largely IT's responsibility, but risk associated with business processes needs to belong to those businesses. Most CIOs and CISOs have, by default, allowed themselves to become ad hoc "insurance underwriters" for implicit risk. Risk acceptance more-properly belongs with the business "owners" of the information assets and business processes. Beyond the realm of IT, it's relatively well-understood that business managers "own" their processes and are accountable for the associated risks and controls. IT is, of course, responsible for helping the business understand the threats to those business processes. The business manager and IT should work together to determine the relative risks and the need for IT-based controls to reduce those risks. In addition, any residual risk should be formally accepted by the business manager.

Unless business decision makers accept this basic principle — and recognize that cuts in security spending can have a negative impact on their objectives — such cuts are all but inevitable.

Four Risk Management Mistakes That Threaten Security Budgets

(1) Taking a "One Size Fits All" Approach to Security and Risk Management

The same level of protection, or the same level of security spending, can't be simultaneously effective and economically viable for each business unit, much less for every component within a single business unit. An optimal level of security spending takes into account the assessed level of risk, avoiding overspending and overprotection. It's well-recognized that the level of security effort needs to be proportional to risk, but attempts to actually follow through can become mired in complexity (see "Toolkit: Enterprise Information Security Architecture Sample Trust Model" and "Toolkit: Conceptual Technology Models for Implementing Security Services"). IT Infrastructure Library (ITIL) V3 requires IT to provide standardized service-level offerings for security and continuity. ITIL V3 is a new standard that isn't yet widely implemented, but it can still provide useful guidance toward the development of security service levels that can align the business with IT. Instead of being forced to specify a bewildering set of technologies and processes for each circumstance, business managers can be offered a relatively small number of risk management profiles that are designed to meet different use cases for data sensitivity and risk.

(2) Making Plans Based on What the Security Organization Wants, Not What the Business Needs

Security professionals have historically made technology-centric investment, implementation and deployment decisions based on what they believe is required, rather than on what the business needs. The flaws in this approach are obvious: The security organization can't expect to understand the business's protection needs — for confidentiality, integrity and availability — if it hasn't asked what they are. Also, there's no reason for the business to accept security budgets that aren't based on what it needs. It's impossible to defend security plans and the budgets they require if they aren't based on business objectives. When IT is unclear about what the business needs, it usually makes the prudent decision to overprotect and overspend. If business managers can't or won't provide information about the risk significance of their business processes, then high-level managers must step in and mediate.

(3) Making Risk-Related Communications Too Complex for the Business to Understand

Security professionals must develop a consistent way to express and articulate the security-criticality of specific IT systems, information assets and business processes. Risk-related issues must be conceptualized in terms that are simple enough for the business to understand — for example, "Whose risk is this?" "Who will benefit from these security protections?" "Who will be affected by a security failure?" Enterprisewide policy must be developed, implemented, and enforced for determining and specifying data criticality. A simple three-level scale — high, medium and low — can provide a common point of reference for articulating the business-criticality of IT, and it can potentially be used for a set of corresponding risk management service levels.

High Risk

- This definitely requires controls beyond baseline protections.
- This requires detailed risk analysis.

- Example: Communications in support of mergers and acquisitions.

Medium Risk

- This may require additional controls (for example, segregation of duties, audit logging and secure backups).
- Risk analysis should be performed, but it's a routine task that doesn't require expert attention.
- Example: Accounting and billing transactions.

Low Risk

- Default-level protections are acceptable.
- Existing baseline should provide adequate protection in virtually all circumstances.
- Example: E-mail.

This simple approach may seem imprecise, but it has proved practical for many enterprises. More-complex four-level and five-level scales are difficult to apply without specialized training, and their use requires considerable discipline. Of course, even a three-level scale can be applied successfully, but only if everyone using it has a consistent understanding of what constitutes high, medium and low risk.

IT risk managers sometimes feel pressured to express risk in quantitative terms. Gartner doesn't recommend creating a fully quantitative risk analysis, but it's usually a relatively practical exercise to express the security impact of a failure within a three- to five-step set of exponential, quantitative bands.

As a hypothetical example, a loss of confidentiality whose impact wouldn't exceed $10,000 could be considered low-sensitivity; one costing between $10,000 and $1 million could be defined as medium-sensitivity; and any impact greater than $1 million could be viewed as high-sensitivity. "Medium" means that a security failure would cost between $10,000 and $1 million, and "high" would be anything anticipated as having more than a $1 million impact. Most individuals can reliably make consistent estimates using such a scale. Of course, monetary values aren't suitable for estimating the criticality of all forms of information resources.

Ideally, business owners should be enabled through a corporate standard risk estimation approach that allows them to make their own assessments of the security needs of these resources (see "Q&A on the Value of Quantifying Risk vs. Qualifying Risk When Communicating With the Business"). Enterprise policy that requires business managers to specify their business needs for data security as part of all requests for new or changed services can be based on simple high/medium/low scales. IT needs to be very clear about the risk control service levels it provides (for example, specifying that corporate e-mail is appropriate only for low-sensitivity data).

(4) Allowing LOB Managers to Transfer Their Risk to the IT Organization and the IT Security Organization

LOB managers are all-too-willing to take advantage of the IT organization's and IT security's willingness (implicit or explicit) to accept residual risks, making the mistaken presumption that IT's "standard offerings" will effectively address any form of IT risk. No matter what type of systems and information they handle, no matter who they share their data with, and no matter what forms of access they allow, LOB managers assume that IT will ensure that security failures don't occur.

Such an approach makes the IT organization or the IT security organization the scapegoat for security failures and any perceived reduction in service or flexibility that's attributed to security technologies or processes. When financial benefits are anticipated, people naturally tend to have a lower perception of the associated risks, so it's only natural for LOB managers to resist security practices that seem likely to slow down or obstruct moneymaking projects.

Furthermore, enterprises often comprise multiple business units, each with its own security policies and architectures, all of which are connected to a common corporate network — and what's beneficial to one business unit might represent a significant risk to another. Counterproductive risk/benefit asymmetries occur when the expected beneficiary of some new project is different from the potential victim of a failure of that project, whether it's IT or a business unit infected by a virus that was introduced by a different business unit. Internal "market forces" can help to align risks with benefits, if all systems and information assets are "owned" by specific business managers who are accountable for any failures in security or continuity.

Conclusion

Several of these mistakes can be easily avoided by agreements between IT operations and risk management staffs. However, complete avoidance of all these mistakes can only take place with the support of business management. Not surprisingly, the LOBs are normally unwilling to accept accountability for IT security risks, unless they're required to do so by upper management. Recognizing that misplaced risk accountability is counterproductive for the business side and the IT side of the equation, executive managers are increasingly willing to mediate to create new policies.

Simple, manageable risk assessment frameworks, explicit acceptance of residual risk, and security SLAs will make it possible to deliver sound enterprise security — and to defend security budgets against cutbacks. The first step that IT risk managers can take toward better alignment with the business is to not treat business managers as a problem that needs to be solved, but rather to regard them as customers who need secure and reliable computing services.

RECOMMENDED READING

"2009 Update: What Organizations Are Spending on IT Security"

"Best Practices in Information Security Before, During and After Employee Downsizing"

"Gartner for IT Leaders Overview: The Chief Information Security Officer, 2009-2010"

"No More Dr. No: Developing a Strategy for Business-Aligned Information Security"

"Is Security a Luxury in a Declining Economy?"

"Key Issues for Risk and Security Roles, 2009"

"Q&A on the Value of Quantifying Risk vs. Qualifying Risk When Communicating With the Business"

"Toolkit: Conceptual Technology Models for Implementing Security Services"

"Toolkit: Enterprise Information Security Architecture Sample Trust Model"

"Transforming From Chief Information Security Officer to IT Chief Risk Officer"

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
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner