Gartner.

G00261249

Digital Business Forever Changes How Risk and Security Deliver Value

Foundational **Refreshed:** 24 August 2015 | **Published:** 10 April 2014

Analyst(s): Paul E. Proctor, Andrew Walls

Mobile, social, cloud and big data, each a disruptive force, together change everything related to protecting systems and information. CROs, CISOs and other risk and security professionals must use the power of risk management and security to deliver value, and to influence business decision making.

Key Challenges

- Digital business takes advantage of technologies that are outside of traditional enterprise control in dynamic environments, with little stability or predictability.
- Risk and security departments are no longer the defenders of the organization; they are the facilitators of a balance between protection and running the business.
- Traditional security technologies have limited applicability in these new environments.

Recommendations

CROs, CISOs, and other risk and security professionals:

- Reset your approach to risk and security to facilitate a balance between the needs to protect the organization, and the needs to run the business.
- Assess and prioritize risks to support conscious choices about what will — and will not — be done to address threats.
- Understand the impact IT risk has on business outcomes.
- Engage all the controls at your disposal, including behavior change, process and technology controls.

Table of Contents

List of Figures

Introduction

This document was adapted from the 2013 Gartner Security and Risk Management Summit keynote presentation, "Reset," given in Washington, D.C., London and Sydney. Demand for risk and security professionals is growing globally. One study of security job postings showed more than 67,000 in 2012 alone, a 73% increase over 2007. Cybersecurity commands a premium of $12,000 over the average for all computer jobs.[1]

Success for a risk and security professional has been traditionally based on having control of the systems and information they protect, but due to cloud, mobile and social, the risk and security role is losing that control. As a result, the profession is going through a dramatic transformation. Risk and security professionals can no longer base their careers and values solely on the technologies and control they can exert. Organizations can no longer assume that by hiring skilled people to run a risk and security program, they are protected.

Transformation is nothing new to risk and security professionals. In the 1960s and 1970s, the security model was entirely centralized. In the 1980s, distributed computing put sensitive data in the hands of business users who knew nothing about IT. In the 1990s, the Internet revolution extended networking to every home through dial-up lines, PCs got cheaper and the Internet made it easier for users to expose sensitive data. The new millennium brought broadband Internet: Every business had a Web presence, and every user had a computer hooked up to the Internet and one at home. During the worm attacks in the early 2000s, organizations suffered more downtime than at any previous period, and real business pain was felt for the first time ever.

During every step of this evolution, the threats have changed. Risk and security skill sets, functions and capabilities have changed with them.

Analysis

Reset Your Approach to Risk and Security, Balancing the Need to Protect the Organization and the Need to Run the Business

Two major changes are facing risk and security teams. The first is that mobile, social and cloud move business data and processes outside of the perimeter, and outside of traditional enterprise control. The second is that these are dynamic environments with no stability or predictability. Managing appropriate levels of risk in this environment will require a new approach. Yesterday it was a new tablet; tomorrow some vice president will ask for email on his new Google Glass.

Traditionally, the value of risk and security has been based on the assumptions that by owning a system, IT could dictate use, and thus, security. But cloud, mobile and social are as easy to engage by end users as starting a browser. While corporate data floods into cloud data centers, many cloud vendors take no responsibility for failure, and promise nothing in terms of security performance. Sometimes, their terms of use even demand ownership of corporate data. If security blocks access, users find a way around the controls. If security says no, many times the business goes ahead anyway.

With respect to information, organizations are increasingly collecting and analyzing data on everything. While this produces great benefits to the business, it creates new security challenges to protect this data and new privacy challenges to guide its appropriate use.

As a result of these new challenges, security and risk teams are resetting how they deliver value. Procurement teams are developing contracts that improve security agreements with cloud vendors, and security managers are improving data classification schemes to make sure that critical data is never in the cloud. Public cloud risks are being managed through better legal agreements, and by aligning data sensitivity with the risks inherent in cloud. Cloud providers themselves are also raising the bar, as their own security is a primary market differentiator, requiring ever higher levels of investment to keep up in the market.

Organizations are supplementing traditional security approaches with new tools, including context-based algorithms for identity management, data isolation through mobile containers, rights management tools and new monitoring capabilities that all enable business benefits while limiting risk (see "Prevention Is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence").

Opening up to social media is forcing risk and security teams to understand how social works, and to develop capabilities in monitoring, data analysis, mitigation and remediation. Social also puts a focus on employee and customer behavior. These risks can't be managed just by buying more technology.

Risk and security teams are optimizing their management strategy and tactics to produce flexible, responsive and scalable programs. New products and services can help, but security teams also have to learn new skills, and to focus on supporting business innovation. Most important of all, they are using risk-based approaches for everything. This means structuring risk assessment processes as enterprisewide programs based on business objectives and processes, not just on IT objectives and processes.

Assess and Prioritize Risks to Support Conscious Choices About What Will — and Will Not — Be Done to Address Threats

As the adoption of cloud, mobile and social accelerates, as digital business emerges, and the Internet of Things becomes reality, complexity will increase and force more changes to the way risk and security operate and deliver value to organizations. These trends will shape how people work and live. Technology will be so natural and pervasive that you won't even need to hold it in your hands.

Knowledge workers of the future will have all of their company, job, family and personal details in a virtual world that is available through any device or app. This will mix traditionally sensitive data with new types including reputation, pervasive video, sensor data, communications and any number of big data possibilities. Social networking, both personal and professional, will be integrated. People will have access anywhere and anytime, so the definition of perimeter will continue to evolve. Vast amounts of information will be collected and processed using the real-time application of constant and pervasive analytics.

Risk and security teams will have to address threats such as board members making the wrong hand gesture at their screen and accidentally tweeting quarterly results. They will have to address a two-speed employee population split between those who grew up in this world, and older employees (over 30) who are adjusting. Teams will need new skills to address new types of challenges, such as how to:

- Identify company versus personal information
- Secure multiple sources
- Authenticate new devices (like wearables)
- Address new types of incidents (like fluctuation in company reputation going public)

- Secure entirely new business models that are emerging from the digital industrial revolution

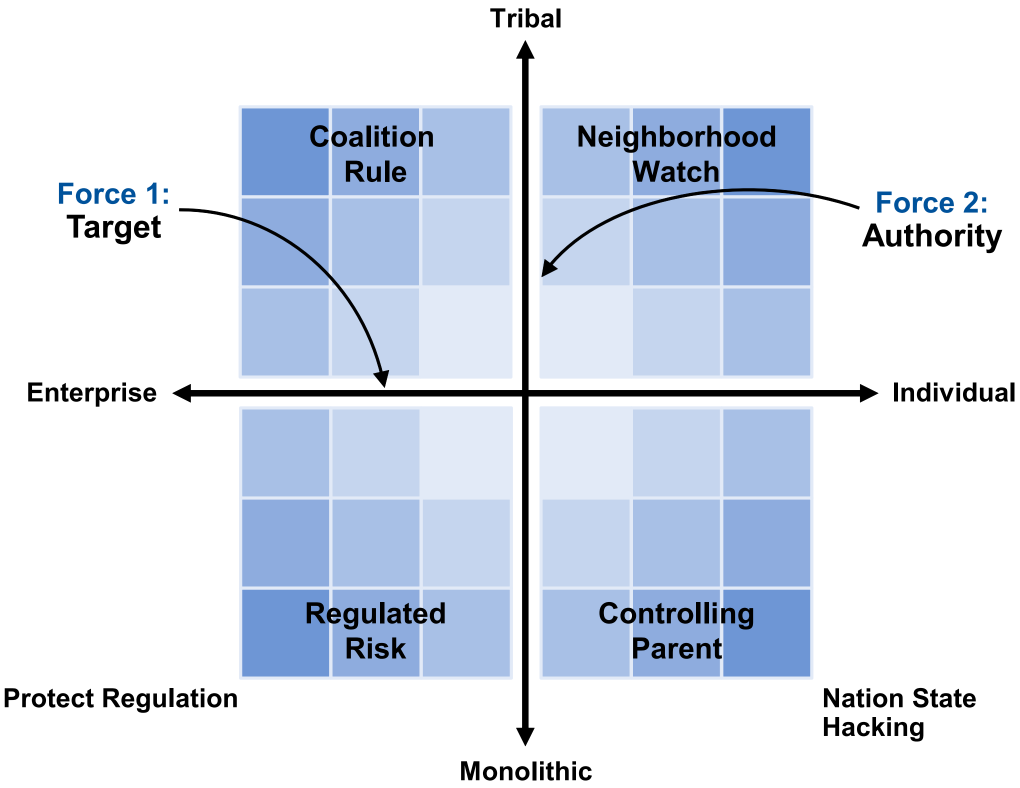
Scenario Planning for Threats

In February 2013, a group of 12 Gartner global thought leaders met in San Diego to share, scrutinize and map the long-term future of security and risk management practices. They conducted a scenario planning exercise to create forward-looking guidance through the year 2020, as illustrated in Figure 1 (see "Security and Risk Management Scenario Planning, 2020").

We looked at two primary forces: who is being targeted, and who has the authority. The first force, the target, spans from enterprises to the individual. Enterprises have traditionally been the target, but increasingly, attacks are occurring via soft targets, individuals, who are employees, customers, and citizens.

The second force, authority, describes control. Authority can represent attackers or protection. This spans across monolithic entities (or governments) to tribal entities (collectives). On the monolithic side, we see government regulation as means to protect, but we also see nation state hacking. Both are forms of authority. On the tribal side, we see consortiums like BITS and Payment Card Industry (PCI) Security Standards Council as a means to protect, but we also see autonomous attacker collectives like Anonymous, LulzSec, or any other number of hacktivism groups.

Figure 1. Gartner Security 2020 Scenario



Source: Gartner (April 2014)

When we lay these forces across each other, it creates four scenarios that your organization will experience over the next decade. Recognizing which scenario matches your reality creates the foundation of new planning guidance:

- **Scenario 1: Regulated risk.** This scenario features strong government authority and enterprise targeting. Governments will attempt to use regulation to provide safety to the enterprise and to itself.
- **Scenario 2: Coalition rule.** There is a continued attacker focus on the enterprise, with a de-emphasis in central authority as rules and regulations are deemed ineffective. We see cartels of autonomous mercenary hackers proliferating, and hacktivism escalates.
- **Scenario 3: Controlling parent.** Increased attacks against individuals will force governments to act. Criminal use of data mining is used to identify potential victims and strong privacy regulations will emerge. The controlling parent is the government who will step in to protect the individual but may also create distraction and limit opportunities for businesses.
- **Scenario 4: Neighborhood watch.** Decreasing regulation signals that government intervention is not going to materially impact the targeting of individuals. E-militias will form to protect against extreme anarcho-hacktivism. Corporate and communal interest groups will flourish.

If these scenarios seem extreme, realize that we have evidence that each and every one of them is happening right now. Reality is always going to lie between the extremes. Most organizations will experience circumstances present in multiple scenarios, but you need to take a step back and figure out which scenarios apply to your organization.

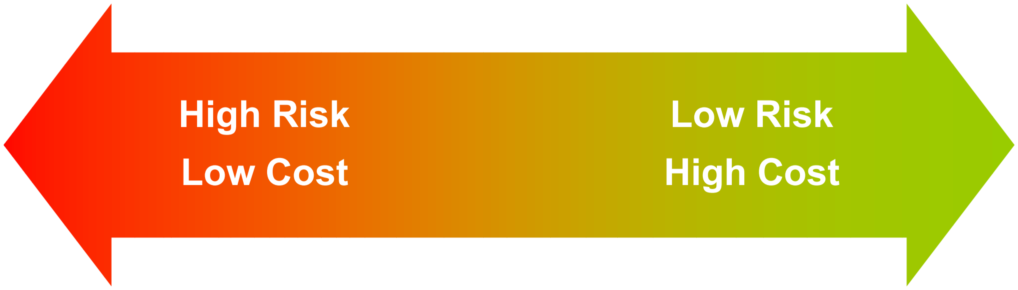
Understand and Communicate the Impact IT Risk Has on Business Outcomes

It has been said for decades that the business owns the risk, but then risk and security teams step in front of business users and tell them they can't do something because it isn't "safe." This perpetuates the idea that the business hired us to take care of the problem, and they need to let us do that. With every action like this, risk and security people tell business "We own the risk."

Risk and security teams are not the arbiters of what is good and bad. They are not the defenders of the organization. Risk and security are the facilitators of a balance between the needs to protect the organization, and the needs to run the business. This axiom holds true, regardless of whether you are a technologist or the chief risk officer (CRO).

There is no such thing as perfect security. Risk posture is a choice. You can either choose to invest more resources and experience less risk, or to spend less resources and experience more risk. Every choice made in IT risk and security influences where the organization is on this continuum (see Figure 2).

Figure 2. Risk and Investment Continuum



Source: Gartner (April 2014)

This reality has ramifications to investment decisions, how budgets are justified, and even how to engage a board of directors. Chief information security officers (CISOs) are their own worst enemy when they position themselves as defenders of the organization, because it lets the executives skate on accountability. Choosing to save some money and experience more risk is a legitimate business decision. The failure is allowing executives to accept risk without making a conscious choice.

Here's a familiar situation. The CISO walks into the CFO's office and says, "I need $1 million to protect the company." CFO: "How much did you spend last year?" CISO: "Nothing." CFO: "And what happened?" CISO: "Nothing." CFO: "Ok, go do that again."

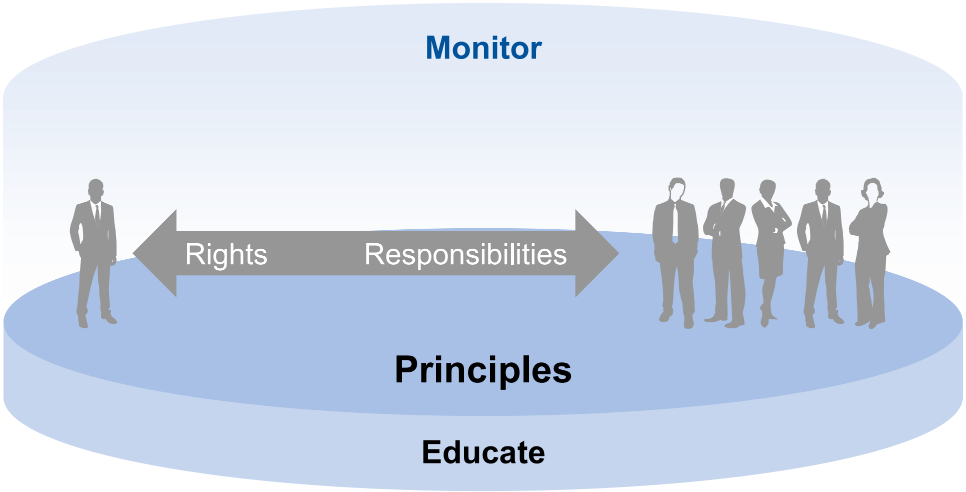
The good news is that you can beat this by changing the narrative. Stop asking for money and start asking for decisions. Explain the reality in Figure 2 to the decision makers, and ask them to commit to their choices, as to where they want to live on this continuum. Saying the risk is owned by the business is not just a platitude. A CISO must have the ability to translate this into reality.

Accept the Limitations of Technology to Protect the Organization

Given that we know we are going to get compromised, we also have to accept the limitation of technology to protect us. Most executives get compromised by clicking on something innocent that leads to computer infection.

In a nexus-driven world, people are empowered. Risk and security professionals can't take that away from them, but they can influence behavior. Gartner is pioneering a technique we call "people-centric security," or PCS, which is the integration of information security and the social sciences (see "Definition: People-Centric Security"). It focuses on encouraging people to make better security decisions by giving them a set of rights and responsibilities, rather than by trying to control them with dictatorial policies and controls (see Figure 3).

Figure 3. People-Centric Security



Source: Gartner (April 2014)

For example, users are given the right to connect their iPads to corporate email, which makes their lives easier, but they are also given responsibilities, such as not storing sensitive data on that iPad. If they violate the responsibility, they lose the right and the convenience of using it for company mail. Essentially, they are motivated to do the right thing for reasons that are meaningful to them.

Benefits to the organization are a reduction in the number of security technologies and an improved risk posture, as people are incentivized to do the right thing. Monitoring controls are critical, because enforcement is about ensuring people are doing what is expected of them, rather than an expectation that technology will force them to do what we want.

Stop Being a Rule Follower and Become a Risk Leader

Organizations must formalize a proactive risk and security program. Organizations with low maturity can be driven by a need to have a list of things to do. In some countries, this is represented by regulatory mandates. In others, it manifests as addressing a framework such as International Organization for Standardization (ISO) 27002. Following the SANS top 20 critical security controls does not equal a good program.

Don't treat security as a check-box exercise with little regard for the real risks the organization faces. Compliance mandates have been in transition for more than a decade to become risk-based, but organizations have not kept pace. Health Insurance Portability and Accountability Act (HIPAA), for example, is a list of risk domains with the requirement to do a risk assessment. Any controls deemed reasonable and appropriate are then required by law. In a 2012 series of spot check audits for healthcare organizations, most failed — not because of a lack of controls, but for the lack of a recent risk assessment to support their control choices.

This risk-based approach gives organizations the flexibility to do what is necessary for their unique situation, and to create a program of controls that actually help the organization succeed. Don't get derailed by regulatory distraction. Gartner recommends proactively selecting controls based on a good risk assessment. Then, identify and address gaps between your chosen controls and external laws or frameworks. Ultimately, compliance should be an outcome of a well-run risk management program (see "Compliance Is No Longer a Primary Driver for IT Risk and Security").

Relate Security and Risk to Business Impact With Executive- and Board-Level Reporting

Non-IT executive interest in IT risk and security, particularly boards of directors, has been on the rise for more than five years. Gartner predicts that by 2014, 80% of large global enterprises will be required to report risk and security posture to their board of directors at least annually. Gartner research shows that most existing board material addressing IT risk and security is not very productive.

To address the recurring issues seen in our research, Gartner published "Toolkit: Board-Ready Slides for Security and IT Risk." This nine-slide deck provides all the concepts that have demonstrated success in front of boards of large enterprises in multiple industries (see also "Building an Effective IT Risk and Information Security Presentation for Your Board of Directors").

Fear, uncertainty and doubt (FUD) has limited value, so don't dwell on it. Many board presentations are largely FUD. Remember, you don't control the threat, but you do control the organization's readiness, and that's a great place to focus the board's attention. You need to abstract out all the technology. While every risk and security subject matter expert will claim to understand this, the vast majority are not executing, leading to a lot of technology-laden, eye chart slides.

Use time in front of the board to bridge the cultural disconnect between them and you. They believe security is a technical discipline, handled by technical people, buried in IT. Instruct them that there is no such thing as perfect security. They don't understand this. Introduce them to their choice to spend more to lower their risk, or spend less and accept more risk.

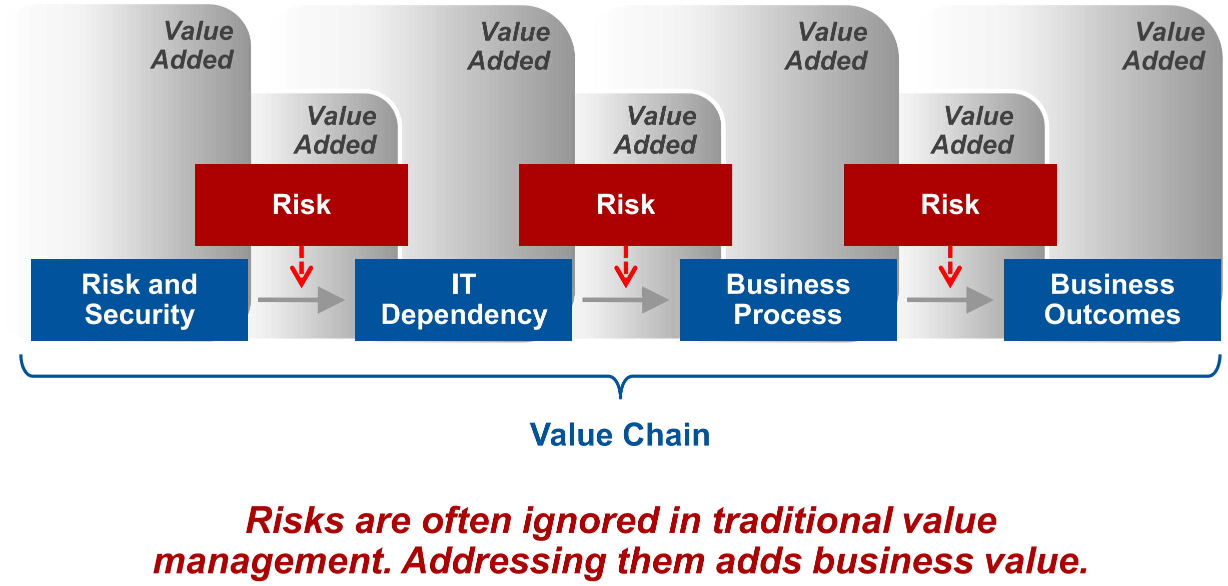
You have to relate security and risk to business impact that the board cares about. Most Gartner clients will readily admit they are extremely challenged to do this.

Integrate Risk and Corporate Performance

Risk and security people in decision-making roles with authority must get better at understanding their own organization's desired business outcomes. Five years ago, Gartner analysts sought an answer to the question "How do you add a business context to risk data?" A collaboration between risk management and corporate performance analysts has resulted in a methodology called Risk-Adjusted Value Management (RVM), which integrates IT risk directly into corporate performance (see "The Gartner Business Risk Model: A Framework for Integrating Risk and Performance").

The essence of RVM is to build causal chains that start on the right with a business outcome, and then build to the left (see Figure 4). First, determine what business processes support the desired outcomes. Then, decide what IT dependencies the business processes have. Finally, identify the security and risk dependencies on IT. The result creates what we call a Risk-Adjusted Value Model, and this can be used to link IT risk and security directly into the achievement of desired business outcomes.

Figure 4. Risk-Adjusted Value Management



Source: Gartner (April 2014)

A proactive approach to IT risk actually adds business value. This is an outcome far beyond simply "aligning with the business." All of this is contingent on understanding your own business. You don't have to go to business school, but you have to understand your own business.

Here's a simple example: A car company in Europe has a manufacturing line where a car rolls off the line every 90 seconds. An hour of downtime caused by IT equals 40 lost cars of inventory. The company reports lost cars, not IT downtime, to its board, because the board cares about cars; it doesn't care about IT.

To be relevant to your non-IT executives, you must understand what decisions your target audience — whether IT operations, the head of applications, the commanding officer, the business unit heads or the board of directors — makes every day. What do you have for them that will influence their decisions?

Reset a Failing Risk and Security Program

Most risk and security organizations are split between security operations and program management. The security operations manager primarily manages technology. The CISO manages the program, with oversight responsibility and most of the decision authority. The operations manager works in IT— and, increasingly, the CISO does *not* work in IT.

This model breaks when the CISO and IT don't get along. This manifests itself in different ways, depending on the organization's structure, but many times it means that the CISO starts making decisions that create issues for IT. This is at its worst when CISOs are highly technical, and do not understand the impacts of their actions on the business. For example, such a CISO might lob blind attacks on the infrastructure, taking down critical business services during working hours, to prove that IT is not secure. This is a real example, and Gartner has seen it multiple times (see "Reset a Security Program That Does Not Work").

In Summary

Risk and security professionals no longer:

- Are responsible for protecting the organization from cyberthreats; they help stakeholders balance the need to protect the organization against the need to run the business.
- Focus exclusively on the technology of security; they engage all the controls at their disposal, including behavior change, process, and technology controls.
- Seek to prevent every possible threat; they assess and prioritize risks to support conscious choices about what will — and will not — be done to address threats.
- Are buried deep in IT; they understand the impact IT risk has on business outcomes.
- Rely exclusively on smart people who know what to do; they formalize their programs with repeatable, survivable and measurable processes.

Stop confusing non-IT stakeholders with IT jargon, and learn to communicate effectively to executives and boards of directors. Use the power of risk management and security to influence business decision making. Today, risk and security professionals have the tools and the understanding to do these things well.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Reset a Security Program That Does Not Work"

"Building an Effective IT Risk and Information Security Presentation for Your Board of Directors"

"Compliance Is No Longer a Primary Driver for IT Risk and Security"

"The Gartner Business Risk Model: A Framework for Integrating Risk and Performance"

"Security and Risk Management Scenario Planning, 2020"

"Definition: People-Centric Security"

Evidence

[1] J. Vijayan, "Demand for IT Security Experts Outstrips Supply," Computerworld, 7 March 2013.

More on This Topic

This is part of two in-depth collections of research. See the collections:

- Security Futures: Plan Now for the Peak Threat and Beyond
- Embed Digital Business Into the Fabric of Your Organization

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."