October 2008

# Cost, Complexity and Risk: Security for the Enterprise of the Future

Contents



## Introduction

According to the IBM landmark Global CEO Study, "The Enterprise of the Future,"[1] Chief Executive Officers and other senior business leaders foresee an exciting new business environment that will be energized and driven by change—including new business designs, disruptive innovation and continuing economic globalization. As a CIO, you are responsible for transforming IT applications, services and infrastructures into nimble, automated environments that will enable your organization to exploit the opportunities of an increasingly dynamic marketplace.

Like many CIOs, you may feel that IT security and compliance could be significant roadblocks to this vision. After all, you're in a position to see how forces of technological change are already driving the spiraling cost and complexity of security and compliance. Change could easily be regarded as the antithesis of security, yet the future is all about embracing even greater change. Questions such as, "How will you ever get full control over risk management and business continuity?" and "How will you improve your adaptability and effectively balance risk, complexity and cost when security and compliance continue to be moving targets?" become top of mind. Chances are, you wish the whole security and compliance issue would simply go away.

For too long, security technology has been developed and deployed apart from the mainstream of IT infrastructures, applications and processes—with little concern from vendors as to how it should be integrated into that mainstream, or how it adds complexity to business processes. It's no wonder that security and compliance costs continue to grow at a rate three times faster than that of IT budgets.

**Highlights**

***The CIO must be an agent of change in the enterprise of the future, while also dealing with how change impacts security and compliance.***

The Enterprise of the Future demands a dramatic transformation of how security and compliance solutions are conceived, applied and managed. This will require the emergence of a new kind of security partner for your organization. This new partner, known as the transformative security vendor, will deliver strong vendor leadership that has long been missing in the security industry. That leadership will include leading-edge security expertise, broad IT expertise, and the deep resources and commitment needed to support a new vision for security and compliance.

That new vision is shared by you and your organization. With your collaboration, your transformative security partner will meet three challenges: 1) to redefine and simplify risk management to provide you clearer guidance in how to balance risk, complexity and cost in a constantly changing environment, 2) to provide a full-scope security framework and portfolio including leading-edge security research, products and services that enable optimum flexibility in deploying comprehensive security solutions that are seamlessly integrated and business driven, and 3) to compress and simplify the risk lifecycle—to reduce security costs and complexity for the long term.

Ultimately, such a transformation tightly integrates security technology into existing IT infrastructure and business processes. This will give you greater control over security as an enterprise asset, and will help make security and compliance simpler, less costly and more accommodating to your evolving business needs.

## The trend: forces of change make IT security/compliance costly and complex

Having converged into a security "perfect storm," five major forces are continuously changing the risk environment, which, in turn, is continuously increasing complexity and costs.

**Highlights**

***Multiple forces of change—both internal and external to the enterprise—have a direct effect on the cost and complexity of security and compliance.***

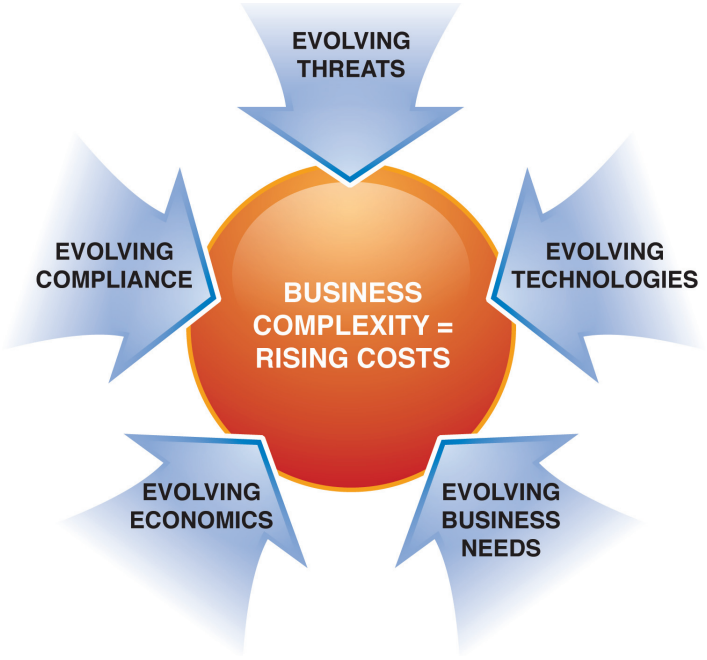


*Figure 1: Five major forces of change*

1. Evolving threats

It wasn't always so complicated. Throughout the 1980s and much of the 1990s, IT security was comprised primarily of antivirus and firewall technology. This relatively narrow technology focus represented the bulk of security budgets. But in more recent years, an entire constellation of threats has emerged, ranging from denial of service attacks, to rootkits, botnets, browser-based attacks, spear phishing and whaling. This rapidly shifting landscape is detailed in the IBM Internet Security Systems™ X-Force® Threat Report.[2] The nature of threats has also evolved beyond mischief to reveal political and profit-driven motives. Most new threats spawn new stand-alone agents or appliances that require expert deployment and management. Even as many of these solutions are gradually standardized and embedded into switches, servers, operating systems and other infrastructure components, new threats emerge, which require new waves of capital investment in new technologies. These new technologies must be funded from budgets that are already strained by the cost of existing security solutions.


*Figure 2: The growing variety of threat species*

2. Evolving compliance

The security-related regulatory and industry compliance burden for organizations also continues to balloon. These mandates are targeted in a variety of ways, including by industry, by country and by state. In many jurisdictions, non-compliance puts companies at risk of civil and criminal penalties. Thus, for senior management, compliance is non-negotiable in the budget priorities debate—usually trumping other security initiatives that compete within the same resource pool.

3. Evolving technology

Virtualization, Web 2.0, service-oriented architectures, cloud computing and other technology evolutions continue to expand the boundaries of the enterprise and establish new avenues of business interaction. Such disruptive innovation also creates new risks and/or undermines legacy security models and investments, which calls for new counter measures and leads to new costs and management challenges for IT.

**Highlights**

4. Evolving economics

Increasingly, security budgets are strained by the dynamics of a globalized economy. Recent fluctuations on Wall Street and worldwide financial markets have dramatically demonstrated how globalization can accelerate and amplify the impact of economic factors ranging from oil process and mortgage rates to currency exchange rates. Even without its most severe ups and downs, the global economy is forcing CIOs to adjust security and compliance strategies and operations. For instance, foreign governments present unique regulatory requirements, global business operations require a 24-hour work day, and security solutions must accommodate a wide range of geographic, language, legal and cultural factors.

5. Evolving business needs

Increasingly, companies have to quickly adjust to changing market conditions. Sometimes it means such strategic moves as mergers or acquisitions, or altering distribution methods. Or it may simply call for creative ways to apply technology, personnel and other assets to boost internal productivity, improve collaboration with suppliers, and enhance interaction with customers. Because all these things typically involve sharing potentially sensitive data, they can impact risk posture.

## The CIO's greatest needs

### Balancing risk, complexity and cost

All the forces of change described above make security and compliance a profoundly difficult and ever-changing puzzle when it comes to planning and budgeting.

***For CIOs, the constant balancing of ever-changing risk, cost and complexity can create security fatigue and ultimately lead to poor choices.***

That's why, despite its enormous importance to the business, IT security/compliance is so often regarded as a distraction and a management burden—one you probably wish would simply go away. But since it is a CIO's unavoidable responsibility, you must seek that elusive point where available budget intersects with manageable complexity and acceptable risk. The task of balancing risk, complexity and cost is made particularly difficult by those five major forces of change that, to a great extent, are also your responsibility.

The business value of data and IT infrastructure has never been higher. As a CIO you must manage a growing array of security measures to protect these strategic assets. But security is only one aspect of your job; you're also responsible for a broad spectrum of other IT imperatives—and your resources are finite.

Given the complexity and relentless cycles of security and compliance challenges, CIOs are prone to "security fatigue" and often take shortcuts to reduce costs and effort.

In some cases, this may mean adopting certain solutions simply to pass compliance audits at the lowest possible cost, while insufficiently mitigating risks. In other cases, CIOs may choose to reduce costs by reducing the number of vendors—often without sufficient analysis of how specific vendors' products and skills align with business needs.

Almost any action taken against cost will have some impact on both complexity and risk.

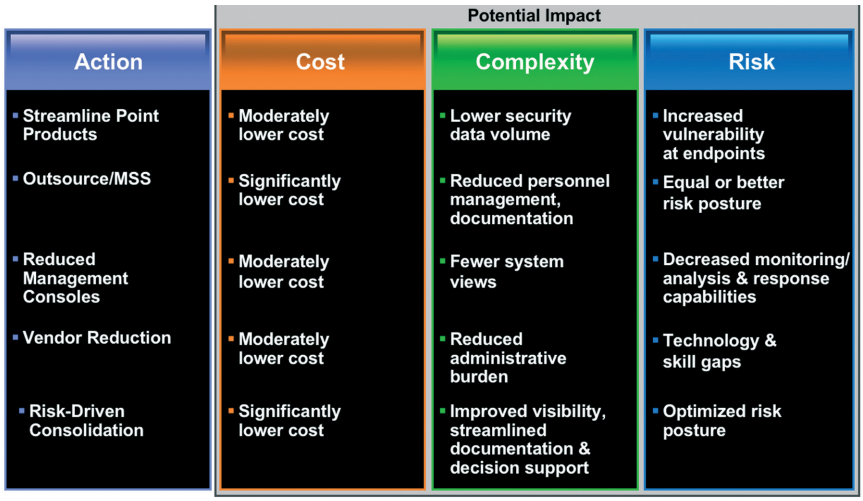


*Figure 3: Actions that mitigate cost of complexity can elevate risk levels*

It will continue to be difficult to balance risk, complexity and cost in a way that yields a responsible approach to solution simplification without security sacrifice or "responsible simplification"—sacrificing security as long as constant changes in the risk and regulatory environment are addressed in an ad hoc manner. For now, quick-fix decisions that are made under pressure may satisfy short-term budget concerns, but will fail to adequately address a lot of risks that have potentially undesirable, headline-making consequences.

So, what can be done to make this balancing act easier? To make choices clearer and more objective driven? We must consider the role of security vendors, and how they have contributed to the current dilemma.

#### Vendor accountability

When it comes to properly balancing risk, complexity and cost, the buck ultimately stops with the CIO and CISO. But to a great extent, responsibility for the frustration and confusion associated with IT security and compliance can be laid at the doorsteps of security vendors. For years, pure-play security companies have created new technologies that are complex and lack interoperability with existing IT systems. The vendors who develop these solutions have had little incentive to make them simpler and less expensive for your benefit.

Then there are infrastructure vendors who assume the mantle of "security provider," but wait until security solutions are mature and largely commoditized before eventually bundling them into switches, servers and applications as features. They generally lack the focused expertise to deliver the most current technology, or to provide you expert guidance on security and compliance strategies.

To date, no vendor from either category has assumed responsibility for reducing total cost and complexity across the full lifecycle of IT security risk. For the most part, you've been on your own. It's time to expect, and demand, much more.

**Highlights**

***The enterprise of the future demands that security and compliance be transformed—from an inhibiting technology to an enabling technology.***

## Meeting security challenges for the enterprise of the future

Your challenge is summarized in an addendum to the IBM Global CEO Study, "The Enterprise of the Future—Implications for the CIO." According to the document, CIOs will be responsible for "driving transformation as 'change leaders' and implementing transformation as 'change agents,' both enterprise-wide as key allies of the CEO and within their own IT organizations."

As a CIO, in order to accommodate and help create the enterprise of the future, you need help in reconciling the conflicts inherent in change. Change may indeed be the force that will drive growth and opportunity, but it also impacts risk—making security and compliance your most vexing responsibility.

To reduce business cost and complexity, risk and compliance management must be more sustainable and consistently business driven in the face of change. Thus, as an IT discipline, security must be transformed—from an inhibitor technology that defines what you can't do, to an enabling technology that empowers you to do whatever your business objectives require.

This is very big job. While there is much that you can do as the change agent within the enterprise, true transformation of security and compliance requires a different breed of security provider.

### The emergence of the transformative security provider

The enterprise of the future requires a vendor that offers the scale and commitment to assume a transformative role in the security industry. Unlike traditional security vendors of any type, the transformative provider will possess the attributes required to guide security technology into the IT mainstream and to assume accountability for the total risk lifecycle:

- *Expertise in every aspect of IT infrastructure*
- *Leadership in security research and development*
- *Depth and breadth of security products and services*
- *Broad integration expertise and business consultation*
- *Expertise in aligning technology with business processes*
- *Global reach*
- *Financial strength and staying power*

**Highlights**

***The transformative security provider must offer a much broader, business-driven set of solutions, along with market leadership and accountability.***

The transformative provider must leverage these attributes to meet three primary challenges:

**1. Redefining and simplifying risk management to accommodate constant change**

As detailed earlier in this document, constant changes in risk posture yield ever-growing lists of security and compliance needs that must be weighed against static budgets. Because CIOs are challenged to get a clear and comprehensive view of their threat postures, they lack guidance in their security decisions. As a result, they often establish priorities that are based on false economies, or are otherwise disconnected from actual business objectives. Part of the problem is simply the lack of information about the various ways those five major forces of change impact risk. Conventional vendors rarely provide insight into more than a single change vector.

To provide you with a complete, business-focused framework for evaluating security needs and spending priorities, the transformative security provider will reintroduce enterprise risk management in a highly refined and dynamic form. It will take all of the major change factors into account, and will include benchmarking processes, maturity models, industry best practices and other elements to generate a more complete and accurate enterprise risk profile that evaluates risk as it impacts actual business objectives.

This is a continuous and adaptive risk management approach that will take much of the pressure and guesswork out of security and compliance planning and management. By enabling smarter, business-driven decisions, it will empower you to better control security-related costs and complexity—not just now, but for the long haul.

**2. Providing a security framework and portfolio that enables seamless, business-focused solutions**

Traditionally, security technology has been developed in isolation, with a narrowly directed purpose, and applied and managed within a narrowly defined silo within the larger IT infrastructure. In a march toward the enterprise of the future, this approach is unsustainable. Major risk challenges (such as Payment Card Industry Data Security Standards) call for technologies in multiple security domains that must be integrated into significant portions of the enterprise infrastructure, and into critical business processes. Cost and complexity cannot be contained if comprehensive solutions must be patched together with technologies from a dozen sources.

The transformative security partner must offer complete security and compliance solutions that are seamless and effective. First, that means a deep portfolio of effective security products that cover five major security domains:

1. People and identity
2. Data and information
3. Application and process
4. Network, server, and end-point
5. Physical infrastructure

Second, the transformative partner must be able to fit the solution to your unique business requirements. This requires deep business and application knowledge, and the resources to integrate the complete technology solution tightly into your unique infrastructure environment and business processes.

Finally, your partner must be at the forefront of security research and development, to keep your security and compliance vision forward looking, and to assure that the forces of change don't overcome your power to counter risk.

Figure 4 provides a simplified view of this total security ecosystem.

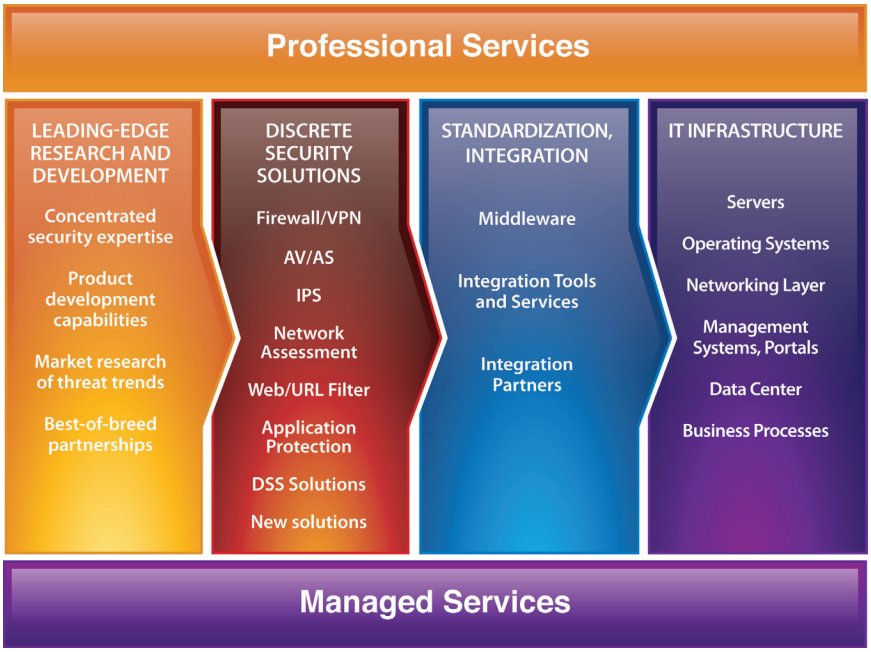


*Figure 4: The total security framework*

**3. Compressing and simplifying the security risk lifecycle**

Is security a product or a feature? The answer is both—over the course of the risk lifecycle. As shown in figure 5, the solution to any specific risk usually begins life as a discrete, stand-alone security product that can be costly and complex. In most cases, the solution undergoes a transition, in which it's standardized over time and eventually becomes a feature that's integrated into the IT infrastructure. As an embedded feature of IT infrastructure, security tends to be less expensive, more mature and more automated in its function.

The transformative provider will compress and simplify this product-to-feature lifecycle in order to give you greater control over security cost and complexity, even as the forces of change constantly alter your risk posture.

First, this means playing an aggressive role in the "transition" stage of the lifecycle—to push security solutions more quickly into the "feature" stage with effective integration techniques, middleware, partnerships and consulting capabilities.

**Highlights**

***In the future, more and more security and compliance solutions must be designed from the outset to be seamlessly integrated into existing IT infrastructure and business processes.***

Secondly, and more important for the long term, the transformative partner will provide a more compressed lifecycle by design. With product development, integration and management capabilities for both security and infrastructure technologies, the new breed of partner will accelerate the process from both ends: 1) by constantly adding more security features and security-enabling frameworks within infrastructure systems, and 2) making security solutions baked-in by design whenever possible, or establishing solution architectures that make security technology easier to integrate into existing IT infrastructures and management systems.

Finally, the transformative security partner will strive to buffer your organization from the disruptive effects of security transformation, and to provide you with greater strategic flexibility by offering many security and compliance solutions as managed services.

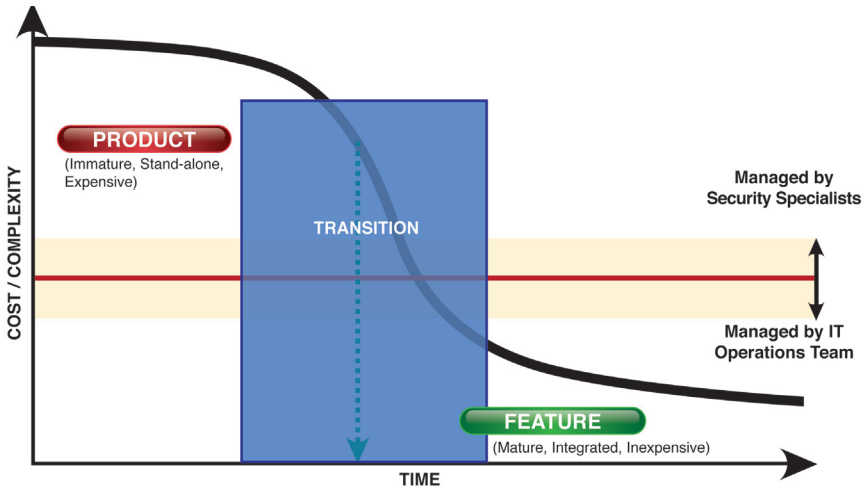


*Figure 5: Cost and complexity diminish over the risk lifecycle. In most enterprises, security solutions can be found at every stage of the lifecycle—product, transition, and feature.*

## Conclusion

Security and compliance of the future must accommodate the enterprise of the future—which will embrace disruptive innovation, globalization and other forces of change that normally make security more complex and costly. The much needed transformation is one that accelerates the transition of exotic new technologies into stable, inexpensive security features that can be easily managed as part of the mainstream IT architecture.

**Highlights**

The point is to eliminate most of the pain and uncertainty of security and compliance management caused by an ever-changing risk environment.

The path is clear and compelling: Migrate security and compliance into the existing IT infrastructure, and integrate with standard management platforms and business processes. Most important: pursue future risk innovations from a total risk lifecycle perspective. This approach is essential in order to reduce the impact of constant change on business cost and complexity, and to improve business continuity.

This is a task that is largely out of your hands: your enterprise can't afford to maintain the specialized personnel required to assess risk posture, integrate new security solutions and maintain all aspects of the constantly shifting risk/complexity/cost equation. And your legacy vendors don't have the resources to offer you a complete solution.

## IBM: the transformative security partner

***IBM is the one organization with the global reach, depth of capabilities and vision to be the market's transformative security partner.***

Securing this dynamic environment is a very big job and demands a very broad and very committed vendor. IBM has the resources, expertise and vision to assume the role of transformative security provider. As the partner that is enabling your enterprise of the future, it makes sense that IBM would be the provider to help you secure it as well. Consider the IBM attributes—which match the requirements described earlier in this document as the essential attributes of a transformative security partner:

- *Comprehensive expertise in IT infrastructure*
- *Leadership in security research and development*
- *Depth and breadth of security products and services*
- *Broad integration expertise and business consultation*
- *Expertise in aligning technology with business processes*
- *Global reach*
- *Financial strength and staying power*

IBM is redefining and simplifying risk management

With market research and analysis, technology development, and hands-on experience in business-driven solutions integration, IBM offers profound insight into the evolution of risk in business environments. Thus we offer a clearer and more complete assessment of the risks you face, and provide more effective security and compliance strategies. For instance, the IBM Client Security Readiness Methodology will help you establish a logical business-driven basis for balancing risk, complexity and cost.

IBM provides the total security framework and solutions portfolio

IBM offers a broad and deep solution portfolio. It spans the five primary security domains and encompasses everything from simple point solutions to comprehensive managed services. Most important, the broad mix of solutions and delivery alternatives give you maximum control, so your strategy can be customized to your unique requirements.

IBM is compressing and simplifying the security risk lifecycle

The IBM security and compliance product roadmap is increasingly guided by the vision of the enterprise of the future, in which IT security accommodates and enables constant change as a matter of course. In product research and development, in strategic acquisitions, and in development of channel and technology partnerships, we seek to make security and compliance solutions a more integrated and effective part of IT infrastructure and business practices.

The enterprise of the future is an exciting destination characterized by constant change. It promises exciting professional challenges—especially in the arena of security and compliance. It's a journey of many steps, but you can be confident that you will go the distance, because IBM will be by your side.

## For more information

To learn more about the security solutions available from IBM to help enterprises reduce risk, cost and complexity by making security/compliance a more integrated and effective part of IT infrastructure and business practices, please contact your IBM marketing representative or IBM Business Partner, or visit the following Web site: **ibm.com**/cio.



International Business Machines Corporation
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
October 2008


[1] IBM Global CEO Study, "The Enterprise of the Future." **ibm.com**/enterpriseofthefuture

[2] X-Force Trend Report - http://www-35.ibm.com/services/us/iss/xforce/midyearreport/

Recyclable, please recycle

CIW03050-USEN-00