

September 25, 2007

The Forrester Wave™: Security Consulting, Q3 2007

by Khalid Kark and Chris McClean
for Security & Risk Professionals

September 25, 2007

The Forrester Wave™: Security Consulting, Q3 2007

PwC And Deloitte Lead The Pack With KPMG Close Behind

by **Khalid Kark and Chris McClean**

with Jonathan Penn and Alissa Dill

EXECUTIVE SUMMARY

Forrester evaluated leading security consulting service providers across 80 criteria and found that PricewaterhouseCoopers (PwC) and Deloitte established themselves as Leaders in the security consulting services market — thanks to their breadth of current offerings and their focus on future growth areas. KPMG International established itself as the next strongest with a rich current offering and solid strategy for growth. Ernst & Young (E&Y) and IBM have good market presence and an established client base but lack the breadth of offerings of the Leaders. Accenture has a strong infrastructure background and is ideal for companies looking to develop a security infrastructure and implementation projects but is not as strong in security strategy. Wipro has a relatively new security practice with impressive growth plans that leverage its existing customer base. BT has a good vision and some good relationships that will enable growth, with success to date focused mostly in EMEA. VeriSign and Verizon Business are relatively small practices with a strong US presence and great customer satisfaction among their clients.

TABLE OF CONTENTS

- 2 **CISOs Need Help In Dealing With Their Evolving Role**
- 4 **Security Consulting Evaluation Overview**
- 7 **The Leaders Have Strong Strategy And Implementation Capabilities**
- 9 **Service Provider Profiles**
- 13 **Supplemental Material**

NOTES & RESOURCES

Forrester conducted services evaluations in July 2007 and interviewed 10 service providers: Accenture, BT, Deloitte, Ernst & Young, IBM, KPMG, PricewaterhouseCoopers, VeriSign, Verizon Business, and Wipro.

Related Research Documents

"Calculating The Cost Of A Security Breach"
April 10, 2007

"US IT Spending Update: Q1 2007"
April 10, 2007

"2007: The Year Of Security Services"
March 23, 2007

CISOs NEED HELP IN DEALING WITH THEIR EVOLVING ROLE

Chief information security officers (CISOs) today are increasingly being asked to go beyond the traditional IT security boundaries of firewalls, networks, and applications. They are being asked to manage the IT regulatory requirements, understand and articulate risks to corporate information, and provide measurements and metrics that would help with governing the organization.¹ And, as if this wasn't enough, threats are becoming a lot more complex and targeted. Many companies simply do not have the resources and expertise to manage all of these facets of information security simultaneously. CISOs are turning to security consulting service providers in large numbers because:

- **Data breaches have created heightened awareness for information security.** Security managers have been complaining for years about not getting enough visibility. Now that data security is a board-level issue, they are not able to answer the tough questions like, “How much should we be spending on security?” and “What are the financial implications of a data breach?” They need help articulating the security story to the executive suite.²
- **Regulatory compliance is a burden.** Most companies went through an overhaul of their financial and IT control environment for Sarbanes-Oxley (SOX) compliance, and soon after found themselves re-inventing the wheel for the Payment Card Industry (PCI) Data Security Standard (DSS) or HIPAA. Enterprises need help developing a comprehensive framework that maps to multiple regulations.³
- **Security measurement and reporting is plagued by deficiencies and inconsistencies.** Many security organizations are at the mercy of the infrastructure and operations teams to provide them with patching and vulnerability information. Periodically they want an external third party to come in and assess those environments and identify gaps.
- **Companies struggle to fully deploy the security technologies they buy.** Many organizations routinely buy security technologies that they don't get around to fully implementing. Typically, this is because of the complexity of the technology, the difficulty of integration, or just because the technology isn't able to deliver on the promised capabilities. Security programs need help with their technology planning and decision-making.

Security Consulting Services Focus On Managing Risk And Integrating Technology

Forrester estimates that total IT services and outsourcing spending has increased by 4% over the past year — to a total of \$76.4 billion today.⁴ Over the past few years, Forrester has seen a steady increase in the number of companies that outsource their security operational responsibilities to managed security service providers (MSSPs).⁵ Over the past two years, some service providers have registered growth rates in excess of 40%. For many service providers, the security consulting practice is relatively new; many traditional security technology vendors and service providers have established small but growing security consulting practices. The majority of security service revenues today come from:

- **Defining and implementing identity and access management programs.** Compliance and managing access to information are the top two drivers for investments in identity and access management services.⁶ Both of these issues become more complex because of extending identities outside the traditional organizational boundaries and the slow but inexorable convergence of physical and logical access controls.⁷ To develop a comprehensive identity and access management (IAM) program, you need to have deep understanding of both the technologies and the business implications. Security service providers are building strong relationships with the technology providers and developing “prepackaged” and integrated solutions for their clients.
- **Performing security assessments and third-party audits.** Almost all security consulting vendors offer security assessment services at competitive rates to get their foot in the door. Assessments give the organization an overview of the security environment, help to identify gaps, and provide recommendations to address those gaps. These assessments trigger larger security projects, where the firm can also help implement those recommendations. Many organizations also tap security consulting firms to audit and assess the security controls of their partners, suppliers, and vendors.
- **Developing control frameworks to manage regulatory environments.** Pursuing compliance with individual regulations is inefficient, time consuming, and costly. Most companies today seek an underlying control framework that they can use to map to multiple regulations. Some of the large security consulting firms have strong audit and control competencies and well-developed control frameworks that map global laws and regulations to them. Some consulting firms specialize in specific regulations like PCI and lead the market in services for those regulations.
- **Developing dashboards to streamline security measurement and reporting.** The crux of the problem is that formal security programs with goals, objectives, deliverables, and SLAs don't exist. As a result, security professionals end up spending a lot of time in a reactive mode.⁸ To be proactive, you need to monitor and measure your security environment; and to institute measurements and metrics effectively, you have to make them part of the process.⁹ All of this requires time and resources that the security team can't afford because it's busy fighting fires. A dashboard/metrics project in isolation is useless unless the consulting firms first help develop the security programs and then define the metrics to measure the performance of the program.

Security Consulting Service Providers Come In All Shapes And Sizes

Many clients pointed to the variance in consultant skill sets even within well-established practices. So most clients undertake the due diligence in selecting consultants but then tend to stick to them for future engagements. Existing relationships also play a huge role in getting security projects. A majority of companies that employ security consulting services have typically used the firm in some other capacity. The current security consulting market primarily consists of:

- **The big four audit firms that dominate the market.** Deloitte, PwC, KPMG, and E&Y are the biggest in terms of security consulting revenues and offer the broadest set of security capabilities.
- **IT infrastructure companies specializing in implementing security.** Accenture, IBM, and Wipro have large security consulting practices, but a majority of revenues come from implementing security as part of broader infrastructure projects. Similarly, companies such as CSC, Tata Consultancy Services (TCS), and Infosys Technologies also do a significant number of security implementations projects.
- **Security product or service vendors.** VeriSign is the only pure-play security vendor that has a comprehensive suite of security consulting services. Other security vendors like Symantec and RSA Security (now part of EMC) have traditionally offered services in conjunction with their product suites but are broadening their consulting practices to include areas outside of their product competencies.
- **Network service providers.** Network service providers are only starting to get into security consulting. Many of them offer managed services, including managed security services. Recent acquisitions of Cybertrust by Verizon Business and of Counterpane by BT have given these providers enough credibility and expertise in this area to compete with traditional security service providers.

SECURITY CONSULTING EVALUATION OVERVIEW

To assess the state of the security consulting market and see how the providers stack up against each other, Forrester evaluated the strengths and weaknesses of top security consulting firms.

Evaluation Criteria Focus On Enterprise-Class Offerings

After examining past research, user need assessments, and provider and expert interviews, we developed a comprehensive set of evaluation criteria (see Figure 1). We evaluated providers against approximately 80 criteria, which we grouped into three high-level buckets:

- **Current offering.** We evaluated market vision, client scores, consultant expertise, and vertical focus. We also evaluated two broad buckets of capabilities: security strategy and security implementation services.
- **Strategy.** We evaluated the integration of security services with other consulting offerings, go-to-market strategy, and future vision and growth plans.
- **Market presence.** We evaluated global client base, consultant coverage, financials, and partnership strengths.

Figure 1 Evaluation Criteria

CURRENT OFFERING	
Value proposition	How does the consulting firm describe the security landscape to clients, and how does it measure the success of its security engagements?
Client and account management	How well does the consulting firm manage engagements? How well do reference clients rate the consulting firm?
Geographic footprint	How does the firm deliver services by geography?
Vertical focus	How broad are the verticals included in the consulting firm's security practice, and how deep are those practice areas in the staff?
Global capabilities and reach	Are all security advisory and implementation services available globally? If not, what are some significant exceptions?
Client engagements	How many client engagements (valued at more than \$50,000) did the firm have in the past year?
Security strategy services	What capabilities does the firm have to provide strategic advice to CISO and executive management?
Security architecture and implementation	What are the firm's capabilities in developing and integrating security solutions and technology architectures for its clients?
Agility in service delivery	Does the firm have the ability to understand and capabilities to serve small, midsize, and large enterprises?
STRATEGY	
Future vision	What is the consulting firm's future vision for its security consulting practice/service?
Go-to-market strategy	What is the primary target market for the firm's security consulting offerings? How does the firm go to market with security? Is the go-to-market strategy through verticals or through other solutions?
Integration with other service offerings	How many of the consulting firm's engagements are accompanied by security consulting services?
Future direction	What are the firm's plans for moving toward its end state vision of security management in terms of intellectual property development, employee qualifications, and geographic variations?
Growth plans	What is the firm's strategy for growth in security management services?

Source: Forrester Research, Inc.

Figure 1 Evaluation Criteria (Cont.)

MARKET PRESENCE	
Client base and engagements	How much have the firm's projects and clients grown in the past year (in number)?
Staff dedicated to security	How many consultants does the consulting firm have dedicated to security on a full-time basis, and what percentage of the overall billable workforce does this number represent?
Financials	What is the firm's financial position and performance?
Partnership strength	What relationships does the consulting firm has with security players?

Source: Forrester Research, Inc.

Evaluated Vendors Have Extensive Capabilities And Experience

Forrester included 10 service providers in the assessment: Accenture, BT, Deloitte, Ernst & Young, IBM, KPMG International, PricewaterhouseCoopers, VeriSign, Verizon Business, and Wipro. Each of these providers (see Figure 2):

- Offers security implementation services as well as security strategy services, and neither one constitutes more than 90% of the total security consulting revenue.
- Has at least \$25 million in security consulting revenue.
- Has at least 50 clients with revenues of more than \$1 billion.
- Performed at least 200 engagements in the previous calendar year and more than 500 engagements in the past three years.

Figure 2 Evaluated Providers: Information And Selection Criteria

Service providers	
Accenture	KPMG
BT	PricewaterhouseCoopers
Deloitte	VeriSign
Ernst & Young	Verizon Business
IBM	Wipro

Service provider qualification criteria

Offers security implementation services as well as security strategy services, and neither one constitutes more than 90% of the total security consulting revenue.

Has at least \$25 million in security consulting revenue.

Has at least 50 clients with revenues of more than \$1 billion.

Performed at least 200 engagements in the previous calendar year and more than 500 engagements in the past three years.

Source: Forrester Research, Inc.

THE LEADERS HAVE STRONG STRATEGY AND IMPLEMENTATION CAPABILITIES

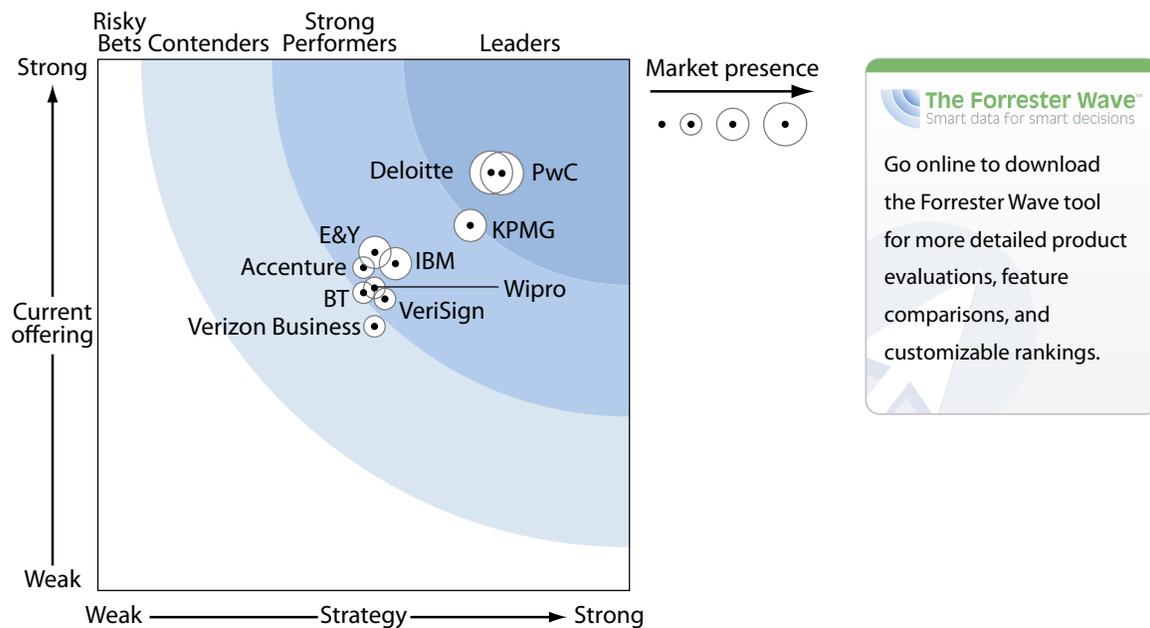
The evaluation uncovered a market in which (see Figure 3):

- **PwC and Deloitte have a formidable lead in all evaluation criteria.** PwC and Deloitte came out on top for each of the three top-level categories: current offering, strategy, and market presence. Both companies have strong global reach, a breadth of services, and extensive experience. Both of these companies are also the largest players in terms of revenue.
- **KPMG has a smaller practice that takes pride in customer service.** The security consulting practice at KPMG is smaller than Deloitte and PwC. It does not have their global reach and depth, but it has a very happy customer base.
- **IBM and E&Y are Strong Performers with a solid customer base.** Both IBM and E&Y pull a large number of their security projects from their existing client base. This has helped them tremendously in growing their security consulting practices. Both companies are now starting to look outside their existing customer base for growth.

- **Accenture and Wipro are strong in large technology implementation projects.** Both firms have large and well-reputed IT outsourcing services. Although Accenture brings in seven times more revenue than Wipro and has a bigger security consulting practice, Wipro's growth in its security consulting services is the highest in the industry.
- **VeriSign is a strong pure-play security consultant with exceptional talent.** VeriSign is a well-established pure-play security vendor that has built a solid reputation over the years. It has one of the most experienced staff in the industry and has consistently scored well on client feedback.
- **BT and Verizon Business have good credibility but little experience.** Both companies have recently focused their energies on security as a strategic offering. Both companies have bought security services companies and have gained the expertise and bench strength, but they need to develop their consulting offerings substantially to compete with the market leaders. Both security consulting practices are new and can't match the bench strength of established players. Both will need to work hard to establish themselves in the industry.

This evaluation of the security consulting market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 3 Forrester Wave™: Security Consulting, Q3 '07



Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Security Consulting, Q3 '07 (Cont.)

	Forrester's Weighting	Accenture	BT	Deloitte	Ernst & Young	IBM	KPMG	PricewaterhouseCoopers	VeriSign	Verizon Business	Wipro
CURRENT OFFERING	50%	3.01	2.78	3.91	3.16	3.05	3.41	3.90	2.72	2.46	2.83
Value proposition	5%	3.00	2.85	3.50	3.05	1.80	2.85	3.70	2.35	2.00	2.00
Client and account management	20%	3.80	3.00	3.70	3.10	3.20	3.80	4.00	3.50	3.40	3.00
Geographic footprint	5%	3.25	3.75	5.00	3.50	5.00	4.50	4.75	1.75	2.25	3.00
Vertical focus	10%	3.50	3.50	4.00	4.00	2.50	3.50	3.50	3.00	2.00	3.00
Global capabilities and reach	5%	3.00	2.00	5.00	3.00	4.00	5.00	5.00	2.00	3.00	3.00
Client engagements	5%	2.00	2.00	5.00	3.00	2.00	3.00	5.00	2.00	1.00	2.00
Security strategy services	20%	1.80	2.20	3.70	2.30	2.70	3.10	3.60	2.30	1.80	2.70
Security architecture and implementation	25%	3.25	2.75	3.70	3.40	3.20	2.90	3.75	2.90	2.65	2.90
Agility in service delivery	5%	3.35	3.35	3.65	4.00	3.65	3.70	3.35	2.60	2.95	3.30
STRATEGY	50%	2.50	2.50	3.70	2.60	2.80	3.50	3.80	2.70	2.60	2.60
Future vision	10%	4.00	3.00	4.00	3.00	3.00	3.00	5.00	2.00	2.00	1.00
Go-to-market strategy	10%	2.00	1.00	3.00	3.00	2.00	2.00	4.00	2.00	2.00	2.00
Integration with other service offerings	20%	2.00	3.00	4.00	2.00	2.00	4.00	3.00	4.00	3.00	2.00
Future direction	40%	2.00	2.50	4.00	2.50	3.00	3.50	4.00	2.00	1.50	2.50
Growth plans	20%	3.50	2.50	3.00	3.00	3.50	4.00	3.50	3.50	5.00	4.50
MARKET PRESENCE	0%	2.87	2.80	4.20	3.19	3.10	3.19	4.14	2.90	2.60	2.98
Client base and engagements	20%	2.25	2.80	4.65	4.10	3.80	3.40	4.60	2.20	2.40	2.30
Staff dedicated to security	30%	2.75	2.25	4.00	2.90	2.95	2.95	4.25	2.25	1.90	3.00
Financials	30%	3.15	3.05	4.55	3.15	2.85	2.90	4.30	3.45	3.50	3.05
Partnership strength	20%	3.25	3.25	3.50	2.75	3.00	3.75	3.25	3.75	2.50	3.50

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

SERVICE PROVIDER PROFILES

Leaders Provide A Strong Mix Of Strategy And Implementation Services

- **PwC is a Leader in security consulting with extensive experience and a great strategy.** PwC offers a mature consulting practice for security, which it views as integrated along with privacy and IT risk management into a single framework. The company has a strong global presence of staff and customers, generally focusing on large-scale engagements. In our evaluation, PwC had the best balance between strategy services and design and implementation services, also

receiving the highest marks for client and account management. The company's security practice did not register the high growth rates of some of the smaller practices, and the firm did not offer some of the managed services for ongoing sustenance, but its scores were generally high in all areas. Large projects requiring a mature business perspective and an even mix of strategy and implementation play well into PwC's strengths.¹⁰

- **Deloitte leads the industry in current offering and market presence.** Deloitte has the largest pool of security consultants in the market, and its global reach includes engagements in more than 100 countries. Security, privacy, and information risk management services within the company are integrated into a single enterprise framework, with a mature perspective focused on client value. In our evaluation, Deloitte's current security offering and market presence took the top spot among all other service providers, although its market strategy score slightly trailed its close rival. Its focus on risk management and privacy and its willingness to invest in R&D activities makes it an excellent choice for those looking for technology expertise coupled with sound strategic advice and strong business orientation. Deloitte brings a pragmatic and mature perspective and is best suited for medium- and large-scale, integrated projects requiring information risk management and security services.¹¹

Strong Performers Focus On Strategy Or Implementation And Do It Well

- **KPMG has good vision and excellent security strategy services.** KPMG's security consulting practice is relatively small compared to many of the large firms it competes with, but it has focused its attention in key capability areas and is poised for substantial growth. Even with a smaller client base, the company's global reach is still very strong, as is its partner ecosystem. In our evaluation, KPMG's overall score in strategic services was higher than its design and implementation services score. The key areas of strength include IT compliance, information risk management, and security assessment and planning. Client satisfaction was also high, especially for nonstandard projects, where the clients said KPMG went the extra mile to make them happy. Companies looking for security strategy services or those with nonstandard project requirements should keep KPMG at the top of their list.¹²
- **IBM has good global coverage and technical credibility.** IBM has one of the biggest security consulting practices in the market, with a robust partner ecosystem and a solid customer base across all global regions. The company expanded its security service capabilities with the purchase of ISS in 2006, although this new group remains a separate organization at this point. In our evaluation, IBM's capabilities in technical design and implementation drew high scores, although it trailed in strategic capabilities, and its perspective of security's role in business was less mature than other large players in the space. IBM has extensive experience in physical security technologies and their implementation. Coupled with its knowledge of information systems, IBM would be a great fit for physical/logical convergence projects. Companies seeking in-depth technical expertise to help with security projects involving large-scale integration efforts should strongly consider IBM.¹³

- **E&Y has a broad customer base with an industry focus.** The number of E&Y consultants dedicated specifically to information security is relatively low compared with competitors of similar size. Much of this practice stems from its audit services; but, like Leaders in this space, E&Y sees security as a crucial element of its clients' overall risk management framework. In our evaluation, E&Y scored well in the design and implementation categories, and unlike its other Big Four cohorts, its strengths are in the more technical fields as opposed to information risk management and IT compliance. These strengths make E&Y a good option to consider for comprehensive implementations of security technologies with consideration for enterprise risk and value.¹⁴
- **Accenture provides technical depth and a business-centric approach.** Accenture ultimately aims to provide the world's leading security consulting services, built on the shoulders of its vast experience in IT consulting. Although not as strong in some of the strategic elements of security consulting, the company scored well across the range of implementation services criteria. In our evaluation, Accenture's scores ended up grouped with those of several other Strong Performers, though it earned high marks for its business-centric vision and investments in continued growth. Companies looking for large-scale security implementation projects with a heavy focus on IT integration should consider Accenture.¹⁵
- **Wipro is unique among large security consulting players in providing an offshoring model.** Wipro's offshoring model is unique among the larger players in the security consulting space. While some customers have mentioned obstacles when working with this model, the cost savings Wipro provides is still a very strong draw for clients. In our evaluation, Wipro's strongest technical capabilities were in application security and identity and access management, with notable strategic capabilities in security sustainability as well. Like other competitors looking to challenge the market leaders, Wipro has a relatively small global presence, but it is experiencing substantial growth in its security consulting practice and is committed to investing in research and recruiting efforts. Companies prioritizing cost savings that are comfortable with the offshoring model should consider Wipro as a viable option for a range of security services.¹⁶
- **VeriSign offers security depth and the most experienced staff in the industry.** VeriSign's security consulting practice is working to complement the company's already strong managed security services group. While not as mature or globally widespread as offerings from competitors in the market, the company's technical capabilities make it an attractive partner for a variety of security implementations. In our evaluation, VeriSign was one of the very few vendors showing strong skills in the wireless and remote access category, with an equal level of expertise in areas such as incident management, threat and vulnerability management, and infrastructure and operations security. VeriSign has a relatively small consulting practice, but it has one of the most experienced consulting staffs, with an average experience of about 10 years. These skills, along with attentive account management, should be important factors in the selection criteria when considering VeriSign.¹⁷

- **BT brings a risk-based approach to all security projects.** BT sees security as a key for businesses operating in a connected world, and it takes a risk-based approach when identifying and scoping such projects. The company's market share in the UK is very strong, although expansion into other parts of EMEA and the rest of the world has been slow. In our evaluation, BT earned top marks for its revenue growth and fared just slightly better in design and implementation services than in strategy services. Both large and small companies — especially those in the UK and Europe — with a need for risk-based security services and expertise in security compliance should have BT on their evaluation list.¹⁸

Contenders Need Experience And Sound Strategy To Move Ahead In This Space

- **Verizon Business has the ability to be a strong services player.** Verizon Business' acquisition of Cybertrust in early 2007 gives the company a competitive offering in the security consulting market, although it is still somewhat unclear whether its focus will be on consulting or managed security services in the near future. In our evaluation, Verizon Business' strongest capabilities were technical in nature, while its perspective on security's role in the business and its strategic services were somewhat lacking. The firm has a long way to go before it can compete with a global presence as large as the Leaders in this space, although it demonstrates a very strong commitment toward customer success and the overall growth of its security practice.¹⁹

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 is an Excel-based provider comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution:

- **Provider surveys.** We surveyed the providers on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed surveys, we conducted calls where necessary to gather details of provider qualifications.
- **Executive strategy briefings.** Once we analyzed the completed provider surveys, we conducted executive strategy calls to clarify and gather further details of provider qualifications.
- **Client reference calls.** To validate product and provider qualifications, we also conducted reference calls with three of each provider's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of providers that meet our criteria to be evaluated in this market. From that initial pool of providers, we then narrow our final list. We choose these providers based on: 1) service fit; 2) customer success; and 3) Forrester client demand. We eliminate providers that have limited customer references and services that don't fit the scope of our evaluation.

After examining past research, user need assessments, and provider and expert interviews, we develop the initial evaluation criteria. To evaluate the providers and their services against our set of criteria, we gather details of service qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the providers for their review, and we adjust the evaluations to provide the most accurate view of provider offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the providers based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update provider evaluations regularly as service offerings and provider strategies evolve.

ENDNOTES

- ¹ Entering 2007, chief information security officers (CISOs) face a siloed security monitoring, measurement, and auditing environment as well as an increased responsibility for protecting the organization's information assets. The challenge of targeted and complex threats and their increased frequency will also contribute to their angst. CISOs are looking for process and cost efficiencies, strategic advice, and specialized skill sets to help them develop and deliver effective security programs. This represents a growth opportunity for managed security service providers (MSSPs), security consultants, and security product vendors. Product marketers at these firms should pump up their outsourcing, consulting, and services offerings to meet this growing demand from CISOs. See the March 23, 2007, "[2007: The Year Of Security Services](#)" report.
- ² Trying to determine the cost of a data breach is no easy task. After calculating the expenses of legal fees, call centers, lost employee productivity, regulatory fines, stock plummets, and customer losses, it can be dizzying, if not impossible, to come up with a true number. In reality, there are many different factors that should be part of the data breach cost calculation — and it's more than just losing money. Although studies may not be able to determine the exact cost of a security breach in your organization, the loss of sensitive data can have a crippling impact on an organization's bottom line, especially if it is ill-prepared, and it's important to be able to make an educated estimate of its cost. See the April 10, 2007, "[Calculating The Cost Of A Security Breach](#)" report.
- ³ For more information on the drivers for adopting frameworks, see the February 24, 2005, "[IT Frameworks For Control And Compliance](#)" report.
- ⁴ Storage hardware and software, infrastructure management software, application servers and business process management (BPM) software, and applications will be the hottest areas of purchase. Servers, communication equipment, operating systems, application development software, and IT consulting services will lag the most in 2007. See the April 10, 2007, "[US IT Spending Update: Q1 2007](#)" report.
- ⁵ Now more than ever, companies have choice in the service providers that can help them secure their IT environment. In fact, more than one-third of companies already outsource at least some of their security operations. See the August 11, 2006, "[Where Do Users Go For Managed Security Services?](#)" report.
- ⁶ New regulations ask subject organizations to obtain greater assurances of authentication. Regulations like SOX, for example, still drive some investment; firms largely understand the requirements and are implementing appropriate controls, but also seek additional identity management solutions that can help them maintain compliance in an efficient manner. See the February 14, 2006, "[Trends 2006: Identity Management](#)" report.
- ⁷ The integration of enterprise physical security controls and management regimes with enterprise IT security architectures is a nascent trend that has been forecast as imminent for several years. But despite the clear benefits to be gained from increased overall enterprise security risk management, the convergence trend is sluggish in taking hold among enterprises. See the August 17, 2007, "[Trends 2007: Physical And Logical Security Convergence](#)" report.

- ⁸ Information security managers around the globe are frustrated. They are struggling to make sense of the reams of data being churned out in today's enterprise environment. The real challenge for them is not only to identify what is important but also to be able to tie this information from disparate tools into business-centric metrics so that the senior executives can understand them, take action, and be confident that the enterprise is secure. Security managers must differentiate between sustainable operational metrics that help them manage and business-centric metrics that are meaningful to top management. To craft the right metrics, information security managers need to subdivide the initiative into three discrete phases. See the March 31, 2006, "[Are We Secure Yet?](#)" report.
- ⁹ In a recent survey, Forrester found that the majority of security metrics programs are still in their infancy or planning phases. The respondents cited two main challenges in developing their metrics programs: finding the right metrics and translating the security metrics into business language. See the May 16, 2007, "[Defining An Effective Security Metrics Program](#)" report.
- ¹⁰ View the vendor summary for more detailed analysis on how PricewaterhouseCoopers fared in this evaluation. See the September 25, 2007, "[PricewaterhouseCoopers Is A Leader In Security Consulting With Great Strategy And Experience](#)" report.
- ¹¹ View the vendor summary for more detailed analysis on how Deloitte fared in this evaluation. See the September 25, 2007, "[Deloitte Is A Leader In Security Consulting With Solid Depth And Global Reach](#)" report.
- ¹² View the vendor summary for more detailed analysis on how KPMG fared in this evaluation. See the September 25, 2007, "[KPMG Is A Strong Performer With A Strong Vision And Excellent Client Satisfaction](#)" report.
- ¹³ View the vendor summary for more detailed analysis on how IBM fared in this evaluation. See the September 25, 2007, "[IBM Is A Strong Performer In Security Consulting Based On Technical Skills And Global Reach](#)" report.
- ¹⁴ View the vendor summary for more detailed analysis on how Ernst & Young fared in this evaluation. See the September 25, 2007, "[Ernst & Young Is A Strong Performer In Security Consulting With Broad Implementation Skills](#)" report.
- ¹⁵ View the vendor summary for more detailed analysis on how Accenture fared in this evaluation. See the September 25, 2007, "[Accenture Is A Strong Performer In Security Consulting With Substantial IT Experience.](#)"
- ¹⁶ View the vendor summary for more detailed analysis on how Wipro fared in this evaluation. See the September 25, 2007, "[Wipro Is A Strong Performer In Security Consulting With Potential For Rapid Growth](#)" report.
- ¹⁷ View the vendor summary for more detailed analysis on how VeriSign fared in this evaluation. See the September 25, 2007, "[VeriSign Is A Strong Performer In Security Consulting. Especially In Key Technical Areas](#)" report.

¹⁸ View the vendor summary for more detailed analysis on how BT fared in this evaluation. See the September 25, 2007, “[BT Is A Strong Performer In Security Consulting, Rapidly Growing With A Heavy UK Presence](#)” report.

¹⁹ View the vendor summary for more detailed analysis on how Verizon Business fared in this evaluation. See the September 25, 2007, “[Verizon Business Is A Contender In Security Consulting With Its Cybertrust Acquisition](#)” report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.