March 18, 2009

# The Forrester Wave™: Information Security And IT Risk Consulting, Q1 2009

by Khalid Kark

for Security & Risk Professionals

March 18, 2009

# The Forrester Wave™: Information Security And IT Risk Consulting, Q1 2009
## Deloitte And PricewaterhouseCoopers Lead, With Accenture Close Behind

**by Khalid Kark**
with Robert Whiteley and Margaret Ryan

## EXECUTIVE SUMMARY

In Forrester's 72-criteria evaluation of information security and IT risk consulting service providers, we found that Deloitte and PricewaterhouseCoopers (PwC) lead the pack because of their superior understanding of business requirements coupled with their deep technical skills. Accenture stands out as a very competent security consulting provider and could pose a significant challenge to the current front-runners. Ernst & Young (E&Y) has vast experience in taking a business view for developing security and IT risk solutions. Wipro Technologies, VeriSign, and IBM offer competitive services but typically excel in niche integration or managed services areas. BT Global Services leads the telcos with superior current offerings while Verizon Business exhibits a slightly better strategy. AT&T still needs to expand its current capabilities and develop a more comprehensive strategy, while T-Systems remains a regional player at best. BearingPoint offers strong public sector capabilities, but clients should invest in due diligence as the company goes through its financial restructuring. Protiviti and Crowe Horwath have smaller practices and offer a viable alternative to the large accounting companies.

## TABLE OF CONTENTS

## NOTES & RESOURCES

Forrester conducted services evaluations in December 2008 and interviewed 15 service providers: Accenture, AT&T, BearingPoint, BT Global Services, Crowe Horwath, Deloitte, Ernst & Young, IBM, PricewaterhouseCoopers, Protiviti, Symantec, T-Systems, VeriSign, Verizon Business, and Wipro Technologies.

### Related Research Documents
"Managing The Expansion Of Security Responsibilities During Economic Uncertainty"
July 3, 2008

"The Forrester Wave™: Managed Security Services, Q4 2007"
October 4, 2007

"The Forrester Wave™: Security Consulting, Q3 2007"
September 25, 2007

## SECURITY AND RISK CONSULTING CONTINUE TO GROW DESPITE ECONOMIC SLOWDOWN

Despite the global economic slowdown and dire projections of a recession or even a depression, information security and IT risk consulting companies have a fairly positive outlook for the future. In fact, many service providers are projecting growth rates in excess of 10%. Forrester estimates that the revenue growth for information security and IT risk consulting will be between 6% and 8% in 2009. After taking into account the service provider revenues and chief information security officer (CISO) spending plans, Forrester estimates that the current size of the information security and IT risk consulting market exceeds $6 billion. Close to 50% of this revenue can be attributed to large accounting firms, such as Deloitte, PwC, and E&Y, and approximately another 20% to IT infrastructure companies, such as Accenture and IBM. Telcos account for another 10%. The rest is split among regional and local information security and IT risk service providers.

### Security And Risk Managers Turn To Service Providers To Help With Their Evolving Role

Today's information security and IT risk managers struggle to keep up with the increasing workloads and dwindling staff. As a result, they are increasingly turning to consulting organizations to get help with:

- **Validating people, process, and technology decisions and strategies.** Many organizations are developing new strategies or updating their existing ones to deal with economic uncertainty. Most commonly, we see CISOs either restructuring their current security organizations to make them efficient or evaluating other ways to reduce spend.[1] All of these decisions require careful consideration and more importantly the experience of having done similar projects before, so that common mistakes and missteps are avoided.

- **Assisting in business transformation projects.** As IT becomes an integral part of the business, protection of information assets becomes a critical issue. Many companies are taking on huge transformational projects that have security implications. Service-oriented architecture (SOA), virtualization, data center consolidation, and information management are all IT projects that will impact the overall security and risk posture of the organization.

- **Developing a strategy to protect firms from security breaches.** Security breaches are increasing not only in number but in magnitude. Corporate executives have moved from worrying about the bad PR of a security breach to a very real set of regulatory requirements and a financial impact that could potentially put the company out of business. In talking to many CISOs, Forrester estimates that the investments around PCI have almost doubled in the past two years for many organizations, and continue to grow.[2] There is so much demand for PCI-related services that many service companies have created a separate PCI practice within their portfolio.

- **Creating process efficiencies.** Many organizations are maturing their information security and IT risk processes and are now looking for ways to create efficiencies or automate existing processes. IT GRC tools are gaining traction because they create these efficiencies.[3] Many service providers are deploying these tools to help companies break down silos of information; have a central repository for audit and compliance information; and, most importantly, reduce the amount of effort to gather, aggregate, correlate, and report this information to various levels within the organization.

- **Dealing with the complexities of identity and access management.** Managing disparate identities across the organization and tying them to appropriate access requirements remains a top challenge. These are typically multi-year, multi-million-dollar projects that require a steady stream of spend with consultancies. Some services firms have come up with unique models where part of the work can be done offshore, or if there is long-term commitment from an organization, the services companies may be willing to invest in the tools/software for the project to share the initial costs.

## Information Security And IT Risk Consulting Continues To Be A Fragmented Market

Security and risk managers are becoming very sophisticated and mature in their services requests and demands. In fact, one service provider commented, "They know exactly what they want, how they want it delivered, and have even done the homework on the price." Yet despite this demand, it's hard to define information security and IT risk consulting, because the answer will vary depending on whom you are talking to and who is offering the service. There is a lot of variance in consultant experience and skill set even within the established and mature practices. The current services market consists of:

- **The Big Four accounting firms that offer deep business and technical expertise.** These firms dominate the revenue as well as the number of people dedicated to information security and IT risk. These firms were the top three in the overall evaluations.[4]

- **Large infrastructure outsourcers gaining momentum due to the current economy.** These players have extensive offshore presence and offer a comprehensive suite of outsourcing services. These companies implement information security and IT risk as part of broader infrastructure projects. Many are reaping the benefits of offering security as an add-on in the current economic climate, where customers are looking to consolidate suppliers.

- **Security vendors looking to services as an enabler of their core products.** These pure-play security vendors have a comprehensive suite of security consulting services. They are well respected and have very good client satisfaction scores.

- **Global audit and consulting outfits as alternatives to the Big Four, but lacking breadth.** They offer a reasonable alternative to the Big Four accounting firms. In fact, some are spinoffs from accounting firms. In general, these firms offer a good understanding of business requirements with an exceptionally strong audit and assessment experience.

- **Telcos that are hard at work to integrate their security offerings and invest in cloud security.** Telcos have varying degrees of maturity in their information security and risk practices, but they all agreed that the future of information security and risk is in the cloud.

## INFORMATION SECURITY AND IT RISK CONSULTING EVALUATION OVERVIEW

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

### Evaluation Criteria: Current Offering, Strategy, And Market Presence

After examining past research, enterprise needs assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated service providers against 72 criteria, which we grouped into three high-level buckets:

- **Current offering.** To evaluate the service provider's current offering, we looked at its consulting capabilities across seven areas: value proposition, client feedback, vertical and geographic footprint, delivery capability, overall consulting service offering, IT risk consulting services, and information security consulting services.

- **Strategy.** To better understand how the provider will execute on its current offering, we measured strategy and vision. Forrester considered criteria including the service provider's future direction, growth plans, and external presence.

- **Market presence.** We evaluated the provider's presence in the information security and IT risk consulting market based on its client base, number of engagements, amount of staff dedicated to information security and risk, and its financial standing.

### Evaluated Vendors Meet Market Presence, Consulting Staff, And Customer Reference Criteria

Forrester included 15 service providers in the assessment: Accenture, AT&T, BearingPoint, BT Global Services, Crowe Horwath, Deloitte, Ernst & Young, IBM, PricewaterhouseCoopers, Protiviti, Symantec, T-Systems, VeriSign, Verizon Business, and Wipro Technologies. Each of these vendors has (see Figure 1):

**Figure 1** Evaluated Service Providers: Service Provider Information And Selection Criteria

| Service providers | Information security consulting | IT risk consulting |
|---|:---:|:---:|
| Accenture | ✔ | ☐ |
| AT&T | ✔ | ☐ |
| BearingPoint | ✔ | ✔ |
| BT Global Services | ✔ | ✔ |
| Crowe Horwath | ☐ | ✔ |
| Deloitte | ✔ | ✔ |
| Ernst & Young | ✔ | ✔ |
| IBM | ✔ | ✔ |
| PricewaterhouseCoopers | ✔ | ✔ |
| Protiviti | ✔ | ☐ |
| Symantec | ✔ | ☐ |
| T-Systems | ✔ | ☐ |
| VeriSign | ☐ | ✔ |
| Verizon Business | ✔ | ☐ |
| Wipro Technologies | ✔ | ✔ |

✔ Service provider participated in this portion of the Wave

**Service provider qualification criteria**

| |
|---|
| Must have at least 25% of information security and risk consulting revenue coming from consulting. |
| Must have at least 50 $1B+ clients overall, with at least 10 $1B+ clients specific to information security and risk projects. |
| Must have completed at least 200 unique information security and risk engagements in the past year and 800 in the past five years. |
| Must have at least 100 dedicated information security and risk consultants spending more than 80% of their time doing information security and risk consulting. |

Source: Forrester Research, Inc.

- **At least a quarter of its revenue coming from consulting.** The service provider must have at least 25% of its information security and risk revenue coming from consulting.

- **Ten or more $1B+ clients of its information security and IT risk consulting.** The service provider must have at least 50 clients whose revenue exceeds $1 billion overall, with at least 10 of these clients specific to information security and IT risk projects.

- **Information security and IT risk engagements.** The service provider must have completed at least 200 unique information security and IT risk engagements in the past year and 800 in the past five years.

- **Dedicated information security and IT risk consultants.** The service provider must have at least 100 dedicated information security and IT risk consultants spending more than 80% of their time doing information security and IT risk consulting.

## FIRMS OFFERING INFORMATION SECURITY AND IT RISK CONSULTING WITH VARIED FOCUS

This year, Forrester endeavored to separate the IT risk-only consultancies from the information security consultancies to compare real peers in both areas.[5] The result was mixed, as many companies define these two terms differently and sometimes even interchangeably. Forrester provided each participant with the domains it would evaluate in each category and had strict requirements in terms of customers, revenue, and consultants to participate in either category.

### IT Risk Consulting Is Dominated By Firms With Rich Auditing And Compliance Backgrounds

The evaluation uncovered an IT risk consulting market in which (see Figure 2):

- **Deloitte, PwC, and E&Y lead the pack in IT risk consulting.** It was not a surprise to see the big accounting firms dominating this space since they are closest to the business and have helped manage IT risk for their financial services clients for a number of years. Deloitte led the pack with established methodologies, thought leadership, and exceptional talent. PwC was not that far behind and has a long heritage of providing pragmatic solutions for IT risk consulting to its clients. E&Y takes pride in delivering a consistent service to its clients in this space.

- **BT, IBM, and Wipro offer competitive options for IT risk consulting.** All three companies have focused on security as a strategic corporate objective and have invested heavily in building IT risk solution sets for their clients. BT is the most mature in its practice in this peer group, while IBM is now focused on harnessing its capabilities across the organization to deliver value to its clients. Wipro is the least mature but continues to be the only large offshore provider that has executive commitment and investment to grow its IT risk practice.

• **BearingPoint's, Crowe's, and VeriSign's IT risk consulting are alternatives to the Big Four.**
All three companies are competing with the Big Four. They offer closer customer interaction —
usually at a cheaper price point — yet at similar levels of professionalism and client focus. They
don't have the breadth in capabilities, bench strength, and global coverage of the Big Four, but
they have established tools and methodologies to help their clients manage their IT risk
effectively.

**Figure 2** Forrester Wave™: IT Risk Consulting, Q1 2009
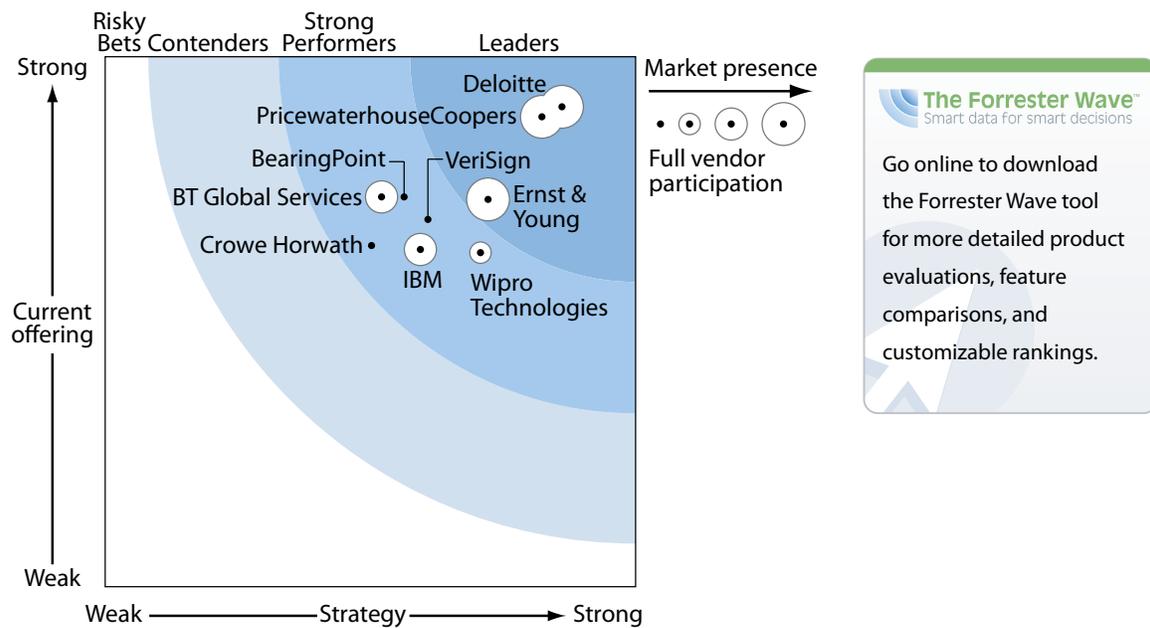


Source: Forrester Research, Inc.

**Figure 2** Forrester Wave™: IT Risk Consulting, Q1 2009 (Cont.)

| | Forrester's Weighting | BearingPoint | BT Global Services | Crowe Horwath | Deloitte | Ernst & Young | IBM | PricewaterhouseCoopers | VeriSign | Wipro Technologies |
|---|---|---|---|---|---|---|---|---|---|---|
| CURRENT OFFERING | 50% | 3.67 | 3.67 | 3.22 | 4.53 | 3.66 | 3.18 | 4.44 | 3.46 | 3.16 |
| Value proposition | 5% | 3.65 | 3.65 | 3.35 | 4.20 | 3.05 | 2.85 | 3.70 | 3.65 | 3.15 |
| Client feedback | 25% | 4.46 | 4.19 | 4.69 | 4.58 | 4.21 | 2.39 | 4.52 | 4.48 | 4.25 |
| Vertical and geographic footprint | 5% | 3.70 | 3.70 | 2.35 | 4.00 | 3.95 | 3.70 | 3.85 | 3.00 | 3.40 |
| Delivery capability | 10% | 2.70 | 2.80 | 1.60 | 4.55 | 3.95 | 4.35 | 4.55 | 2.25 | 3.25 |
| Overall consulting service offering | 19% | 2.90 | 4.25 | 2.65 | 4.35 | 3.00 | 3.50 | 4.35 | 3.40 | 2.40 |
| IT risk consulting services | 36% | 3.80 | 3.25 | 3.05 | 4.70 | 3.60 | 3.20 | 4.60 | 3.15 | 2.75 |
| | | | | | | | | | | |
| STRATEGY | 50% | 2.89 | 2.67 | 2.58 | 4.37 | 3.67 | 3.04 | 4.18 | 3.12 | 3.61 |
| Future direction | 30% | 3.50 | 3.00 | 2.50 | 4.50 | 4.00 | 4.00 | 5.00 | 2.50 | 2.50 |
| Growth plans | 60% | 2.40 | 2.40 | 2.60 | 4.20 | 3.40 | 2.40 | 3.80 | 3.40 | 4.20 |
| External presence | 10% | 4.00 | 3.30 | 2.70 | 5.00 | 4.30 | 4.00 | 4.00 | 3.30 | 3.40 |
| | | | | | | | | | | |
| MARKET PRESENCE | 0% | 1.76 | 3.11 | 1.13 | 4.90 | 4.09 | 3.34 | 4.83 | 1.84 | 2.59 |
| Client base and engagements | 25% | 2.15 | 3.05 | 1.00 | 5.00 | 4.35 | 4.05 | 4.70 | 2.15 | 3.25 |
| Staff dedicated to information security & risk | 25% | 2.50 | 2.60 | 1.90 | 5.00 | 4.00 | 4.10 | 5.00 | 2.80 | 3.10 |
| Financials | 50% | 1.20 | 3.40 | 0.80 | 4.80 | 4.00 | 2.60 | 4.80 | 1.20 | 2.00 |

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

Source: Forrester Research, Inc.

## Accounting Firms Lead Information Security Consulting; Systems Integrators Are On The Rise

We also assessed the information security consulting market independently of the IT risk consulting offerings. There were some common players across both categories, but the evaluation uncovered a somewhat different landscape (see Figure 3):

- **Accenture, Deloitte, E&Y, and PwC are the leaders in information security consulting.** It may come as a surprise to some that the big accounting firms have very strong capabilities in security consulting. This is consistent with the feedback we receive from CISOs who seek out the big accounting firms for their technical depth. Over the past few years these companies have built very deep and solid technical capabilities. The only other company that was not a Big Four accounting firm and scored really well in this category was Accenture. Not only does the company offer a great value proposition to its clients through its seamless onshore-offshore

model, but it has the technical capabilities to offer real end-to-end security services. It has built excellent relationships with its partners and continues to drive business.

- **BT, IBM, and Wipro offer competitive solutions and are gaining ground.** All three companies have excellent capabilities in specific domains of information security. BT is great at doing quick assessments, IBM's strength is in its global footprint and breadth of services, while Wipro offers great technical insight and willingness to work with its customers. All three have well-established partner relationships that enable them to offer pretested and integrated solutions — a pain point for many CISOs in the past.

- **Verizon Business, Symantec, and Protiviti security services are still establishing themselves.** All three practices are relatively small and less well-established than some of the market leaders but have shown a lot of promise in the delivery of security services. All three have significant plans to expand the size and scope of their existing service offerings to serve their clients better. And if they execute well on their respective visions, they will be a strong force in this segment.

- **AT&T and T-Systems lag the pack but are still contenders.** AT&T and T-Systems have a heritage of working on security issues and value research and innovation in information security, but both of these companies are very focused on their core business, and security consulting is delivered in the context of their telco business. Forrester found these practices to be less mature than some of the leaders and too focused on security technology.

This evaluation of the information security and IT risk consulting market is intended to be a starting point only. We encourage readers to view detailed service evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

**Figure 3** Forrester Wave™: Information Security Consulting, Q1 2009

Source: Forrester Research, Inc.

**Figure 3** Forrester Wave™: Information Security Consulting, Q1 2009 (Cont.)

| | Forrester's Weighting | Accenture | AT&T | BearingPoint | BT Global Services | Deloitte | Ernst & Young | IBM | PricewaterhouseCoopers | Protiviti | Symantec | T-Systems | Verizon Business | Wipro Technologies |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CURRENT OFFERING | 50% | 4.04 | 2.74 | 3.51 | 3.89 | 4.37 | 3.63 | 3.39 | 4.28 | 3.50 | 3.10 | 2.94 | 3.24 | 3.27 |
| Value proposition | 5% | 4.70 | 2.70 | 3.65 | 3.65 | 4.20 | 3.05 | 2.85 | 3.70 | 3.85 | 2.85 | 2.85 | 3.00 | 3.15 |
| Client feedback | 25% | 4.25 | 4.34 | 4.46 | 4.19 | 4.58 | 4.21 | 2.39 | 4.52 | 4.54 | 4.41 | 4.43 | 4.43 | 4.25 |
| Vertical and geographic footprint | 5% | 3.75 | 2.35 | 3.70 | 3.70 | 4.00 | 3.95 | 3.70 | 3.85 | 3.15 | 2.35 | 1.90 | 2.85 | 3.40 |
| Delivery capability | 10% | 3.65 | 0.70 | 2.70 | 2.80 | 4.55 | 3.95 | 4.35 | 4.55 | 2.05 | 2.05 | 2.20 | 2.00 | 3.25 |
| Overall consulting service offering | 19% | 4.15 | 2.65 | 2.90 | 4.25 | 4.35 | 3.00 | 3.50 | 4.35 | 3.35 | 2.65 | 1.65 | 2.65 | 2.40 |
| Info. security consulting services | 36% | 3.90 | 2.30 | 3.35 | 3.85 | 4.25 | 3.50 | 3.80 | 4.15 | 3.25 | 2.85 | 2.95 | 3.15 | 3.05 |
| | | | | | | | | | | | | | | |
| STRATEGY | 50% | 3.95 | 2.49 | 2.89 | 2.67 | 4.37 | 3.67 | 3.04 | 4.18 | 2.49 | 3.04 | 2.34 | 3.21 | 3.61 |
| Future direction | 30% | 4.00 | 2.00 | 3.50 | 3.00 | 4.50 | 4.00 | 4.00 | 5.00 | 2.50 | 2.50 | 2.00 | 2.50 | 2.50 |
| Growth plans | 60% | 3.80 | 2.60 | 2.40 | 2.40 | 4.20 | 3.40 | 2.40 | 3.80 | 2.40 | 3.20 | 2.40 | 3.60 | 4.20 |
| External presence | 10% | 4.70 | 3.30 | 4.00 | 3.30 | 5.00 | 4.30 | 4.00 | 4.00 | 3.00 | 3.70 | 3.00 | 3.00 | 3.40 |
| | | | | | | | | | | | | | | |
| MARKET PRESENCE | 0% | 2.61 | 1.33 | 1.76 | 3.11 | 4.90 | 4.09 | 3.34 | 4.83 | 1.19 | 1.94 | 2.34 | 2.53 | 2.59 |
| Client base and engagements | 25% | 2.15 | 1.40 | 2.15 | 3.05 | 5.00 | 4.35 | 4.05 | 4.70 | 1.95 | 2.55 | 2.55 | 2.50 | 3.25 |
| Staff dedicated to info. security & risk | 25% | 3.50 | 1.90 | 2.50 | 2.60 | 5.00 | 4.00 | 4.10 | 5.00 | 2.00 | 2.00 | 2.40 | 2.40 | 3.10 |
| Financials | 50% | 2.40 | 1.00 | 1.20 | 3.40 | 4.80 | 4.00 | 2.60 | 4.80 | 0.40 | 1.60 | 2.20 | 2.60 | 2.00 |

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

Source: Forrester Research, Inc.

## VENDOR PROFILES: IT RISK CONSULTING

### Leaders

- **Deloitte.** Deloitte has the largest global information security and IT risk services practice. Deloitte offers the best of both worlds by not only having an excellent understanding of the business, but by also having the ability to integrate an IT risk mindset and a deep technical expertise into its engagements. The firm has established itself as a global leader in offering complex, large-scale information security and IT risk services. Deloitte continues to invest in resources and establish centers of excellence in areas such as identity and access management (IAM), data protection, and application security. Deloitte also had the highest growth rate of 21% in FY08.

- **PricewaterhouseCoopers.** PwC has one of the largest information security and IT risk practices globally. The firm has a long history of innovations in this space and continues to be a significant presence with pragmatic solutions. PwC is ideally suited for organizations that want to view IT risk from practical and holistic views and take them from assessment through to implementation. PwC's strength is to connect these capabilities, based on its vast expertise in this space. PwC differentiates itself by offering its clients a globally consistent service through its network of firms around the world, its partnerships across geographies, and its capacity to work with clients who have operations in all areas around the globe. In spite of the economic slowdown, PwC continues to show healthy growth rates in several domains and geographies. The firm plans to grow in the future by focusing on areas such as a continued investment in its information security and IT risk practices. PwC plans on enhancing its capabilities in strategy, identity management, and information protection/management.

- **Ernst & Young.** E&Y focuses on the business risk and helps its clients understand key business processes and then establishes what applications and technologies support those processes. As a result, the practice is heavily involved in helping with selection, design, and implementation of GRC tools. E&Y is a good fit for organizations looking for a global services partner with strong IT risk capabilities and an exceptional audit and assessment heritage. E&Y's information security and risk practice has had a healthy growth, with 16% growth in revenues for the year ending June 2008. E&Y plans to grow its information security and IT risk practice by thoroughly penetrating its own service offerings and expects to grow in all major geographic markets. Some of its strongest growth comes from Asia Pacific (APAC) and Europe, Middle East, and Africa (EMEA).

## Strong Performers

- **BT Global Services.** BT not only has a strong presence in Europe but already has a substantial presence in the US market, with more than 700 clients. The company is expanding in the North American security services market by acquiring companies such as Counterpane (MSSP) and INS (consulting). Its approach includes providing information security consulting in a modular fashion, where it offers a fixed-priced quick assessment called a "Quick Start," to get its foot in the door. BT is excellent for organizations that are looking for an established information security consulting player with a risk-focused approach and a broad experience. Organizations can evaluate the services and establish trust via a Quick Start engagement, and, once comfortable, move on to bigger and more complex projects. This approach has been extremely popular given the current economic conditions.

- **IBM.** IBM plans to grow this practice by truly integrating security into its various business areas and offering it as a cohesive function of those business areas. IBM has taken on a companywide initiative to articulate its governance and risk management (GRM) vision to clients and make the disparate pieces work together. IBM continues to be a strong force in this area due to its strong individual components.

- **VeriSign.** VeriSign's consulting practice offers an established standalone security company that may not be as big as some of its competitors' practices, but it offers good technical capabilities coupled with a deep understanding of the IT risk domain. VeriSign boasts a highly skilled staff with an average industry experience of 12 years for its consultants. Due to some uncertainty around its divestiture, this practice area has not grown in line with the company's capabilities. VeriSign is ideal for companies looking for a pure-play security service provider offering a breadth of experience and a solid alignment with its managed services arm. VeriSign also offers its clients threat intelligence through its well-respected iDefense offering. VeriSign plans on growing in the future by continuing to invest in its PCI practice as well as by integrating its capabilities with the managed services and threat intelligence parts of the business.

- **Wipro Technologies.** Wipro is still building out its enterprise risk management capabilities, and its overall risk practice is not as mature as some of its competitors', but it has strong partnerships in IT GRC and continues to invest in enhancing its capabilities in this area. Companies looking to integrate their technologies and process for IT GRC should take a look at Wipro.

- **BearingPoint.** BearingPoint offers a laser-focused vision to its clients for information security and IT risk consulting. It will not likely take on a project if it can't find a way to factor in how the information security and IT risk consulting will reduce cost, reduce complexity, or provide improvement. BearingPoint offers a unique mix of management and technology expertise where it serves purely as management consultant for some clients and technology consultant for others. The company's risk and compliance practice is focused on business impact and building audit and compliance requirements into the security program.

- **Crowe Horwath.** Crowe has established itself as an emerging alternative to the Big Four accounting firms. It operates in North America only but has member firms across the globe as part of the Horwath International network. The company has a heritage in financial control auditing and Sarbanes-Oxley (SOX) engagements. Working in the financial services sector gave it the credibility to work with the business side on compliance issues while improving the overall security posture for its clients. Crowe would be ideal for companies looking for cost-effective assessment services, IT general control reviews, and security reviews, including physical security. Crowe has created some nifty tools to cut down the expense of doing assessments and provide consistency in results across the organization. It's counting on these efficiencies to help it offer greater value to clients and provide significant growth for the company in the current economic climate.

## VENDOR PROFILES: INFORMATION SECURITY CONSULTING

### Leaders

- **Deloitte.** Deloitte stands as the leader in information security consulting as well, due to its depth and breadth of services, and, most importantly, because Deloitte is able to seamlessly integrate its understanding and knowledge of the business with its delivery capabilities in the security business. Deloitte also offers a very robust operational security capability that is currently being deployed in various public sector projects.

- **PricewaterhouseCoopers.** PwC has always led the way in developing and delivering the methodologies and practices that are consistent with the current market conditions. Along with its business applications practice, PwC has a strong identity and access management (IAM) practice that enables its clients to reap the benefits from tight partnerships with ERM vendors.

- **Accenture.** The security practice at Accenture has been growing rapidly over the past few years, but 2008 was exceptionally strong, with Forrester estimating growth at more than 40%. Accenture shines in large and complex IT infrastructure and integration projects. The company has significantly increased its R&D spend for 2009 and continues to invest in developing services to meet the changing economic climate. Accenture not only analyzes the problems but specializes in offering pragmatic solutions to those problems. It offers deep technical expertise and strong vendor relationships. Accenture plans on continuing its growth trajectory by focusing on integrating its existing security services with other parts of its business such as its outsourcing, risk management, and infrastructure practices.

- **Ernst & Young.** E&Y's security practice provides strong and consistent integration capabilities. Some of its strongest growth comes from APAC and EMEA where it has been responsible for some large-scale infrastructure and integration projects.

### Strong Performers

- **BT Global Services.** BT security consulting has a mission to grow BT's core business and therefore will expand in areas that are strategically aligned to that core business — such as cloud computing and infrastructure on-demand — that drive professional services, whether upfront or contractually ongoing. BT plans on enhancing its cloud security offerings and associated consulting services.

- **IBM.** IBM has the technical capability and the range of services that match those of its best information security and IT risk competitors, but IBM struggles to articulate this depth and breadth and deliver the full extent of its capability due to its size and business unit focus. IBM is well-diversified globally, with a revenue distribution of 40%, 30%, and 30% from the Americas, EMEA, and APAC, respectively. IBM is ideal for companies looking for a service partner that offers efficiency and cost reductions in the overall infrastructure and that also integrates security

in the solutions, rather than a purely security-focused firm. IBM has a well-respected managed security services (MSS) offering in addition to the consulting services. The MSS revenue is currently twice as much as pure consulting revenue and is growing at a much faster rate as well. IBM plans to grow this practice by truly integrating security into its various business areas and offering it as a cohesive function of those business areas.

· **Wipro Technologies.** Wipro continues its rapid expansion in the European and North American markets. Not only has it grown at a breakneck pace in these markets, but it still plans on growing more than 100% in the security practice in 2009. Wipro has set itself apart from other offshore providers with its emphasis on security. Wipro is ideal for organizations looking for a mix of onshore and offshore capabilities and companies that are comfortable with offshoring some or all of their tasks. Wipro does provide a unique value proposition to its clients by taking on multi-year commitments and passing on the cost benefits to its clients.

· **Verizon Business.** Verizon Business has fully integrated its Cybertrust acquisition and is now focused on integrating information security consulting in all its service offerings, where it is well ahead of other telcos. Verizon has had phenomenal growth in the areas of PCI and IAM — these areas bring close to 40% of the services revenue for Verizon Business. The firm is ideal for a company that is: 1) looking for a service provider to offer integrated security solutions, including cloud-based security solutions, or 2) looking for deep PCI and forensic capabilities associated with data breaches. The firm plans to grow in the future by focusing on delivering integrated security capabilities to its clients through its newly established global services organization.

· **BearingPoint.** A vast majority of the firm's information security and IT risk consulting revenues comes from public sectors (73%) and financial services sectors (approximately 18%). Consequently, BearingPoint is ideal for Fortune 1000 organizations in financial or public services organizations requiring complex design and integration capabilities such as identity management and biometrics. BearingPoint plans on investing in more verticalization of its solutions to grow its business.

· **Symantec.** As a product company, Symantec often tends to get into a transactional mode. Services play a key role in maintaining the relationship with the customer and help get influence within customer accounts. Symantec offers a practical perspective: Come in at a competitive price point and let customers take on bite-size chunks. Symantec security services has a unique model where its professional services are divided into three categories: advisory, residency services (on-site advisory and product support), and enablement services (product maintenance and support). Symantec claims that 60% of its services revenue comes from advisory services. The company is ideal for organizations that have an existing Symantec deployment and are looking for advice in other peripheral areas. North America is still its biggest region, but EMEA is growing at a healthy pace and is not that far behind the Americas. Symantec also has offshore

capabilities through two centers in India, which it started for its MSS practice but to which it has since added consulting capabilities.

- **Protiviti.** Protiviti is a well-established and well-respected player in the security market. The company focuses on building tools and methodologies for integrating clients' compliance and audit requirements and aligning them with a holistic view of the organization's risk posture. The firm also has deep technical and tactical expertise to implement the regulatory mandates. The firm is an established thought leader on IT compliance issues with respect to regulations such as HIPAA and PCI. Its partnerships with other Robert Half International subsidiaries give it a global footprint and reach. It serves 35% of the Fortune 100 companies and 25% of the Fortune 500 companies. It is ideal for organizations looking for focused IT risk consulting services and a solid understanding of the audit and compliance market.

## Contenders

- **AT&T.** AT&T information security consulting services focus on protecting the end-to-end network. The consulting services are primarily used to determine requirements and develop strategy and road maps around the security measures for AT&T clients. AT&T values innovation and has a heritage of bringing new cutting-edge technologies to its clients. A majority of the information security services revenue comes from managed services. AT&T is ideal for North American companies looking to focus on network-centric security or use a well-respected name in specific areas such as penetration testing or security architecture review. Companies looking for cloud-based security offerings and solutions should also look to AT&T.

- **T-Systems.** T-Systems offers a wide breadth of infrastructure security services primarily in EMEA and is especially strong in Germany. Its information security solutions are primarily divided into three areas: IAM, enterprise security management, and telecom infrastructure security. All three service lines offer consulting, integration, hardware and software, management, and maintenance (e.g., plan, build, supply, run). T-Systems is ideal for companies looking for large, technically complex projects in EMEA that require deep infrastructure integration and deployment capabilities, such as the electronic toll collection project in Germany, for which T-Systems handled all of the security and encryption key management. T-Systems plans to grow this area from the existing 30% of its services business by focusing on the infrastructure projects it takes on and integrating security into the mix.

## SUPPLEMENTAL MATERIAL

### Online Resource

The online versions of Figure 2 and Figure 3 are Excel-based vendor comparison tools that provide detailed product evaluations and customizable rankings.

### Data Sources Used In This Forrester Wave

Forrester used a combination of two data sources to assess the strengths and weaknesses of each service provider:

- **Service provider surveys.** Forrester surveyed service providers on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed service provider surveys, we conducted service provider calls where necessary to gather details of service provider qualifications.

- **Customer reference surveys.** To validate offerings and service provider qualifications, Forrester also conducted an online reference survey for at least five of each service provider's current customers.

### The Forrester Wave Methodology

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

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor 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 vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we encourage readers 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 vendor evaluations regularly as product capabilities and vendor strategies evolve.

### ENDNOTES

[1] One of the biggest challenges facing IT decision-makers today is balancing the cost of security measures against risks that are becoming increasingly sophisticated, common, and devastating. IT services clients increasingly bundle security services into their comprehensive outsourcing deals with major full-service providers like IBM, Northrop Grumman, and Wipro. Managed security services (MSS) now account

for more than $3 billion a year of major service provider revenue, and business growth is accelerating as IT clients continue to sharpen the focus on security. To help IT managers make better provider choice decisions for managed security services, Forrester surveyed 14 of the largest global comprehensive IT service providers about their current offerings. We found that managed security services will be a major IT theme for 2008 — leading to rapid growth of MSS bundled into broader service offerings that include consulting as well as long-term services. Clients now have more options to choose from in selecting a managed security service provider with good solution alignment to business strategy and requirements. See the July 7, 2008, "IT Outsourcers Enhance Buyers' Options For Enterprise Managed Security Services" report.

[2]    PCI (Payment Card Industry) compliance — a requirement for accepting credit card transactions — can be difficult. About 65% of global enterprises are still working on their PCI compliance initiatives. But PCI compliance is an ongoing effort, not a bounded IT security project. Insight into the process and the role of the qualified security assessor (QSA) can make it easier, while implementing standard security best practices upfront will ease the pain when the on-site audit begins. See the September 11, 2008, "Confessions Of A QSA: The Inside Story Of PCI Compliance" report.

[3]    At a time when the global business community struggles to enhance internal controls and maintain long-term viability, improvements in governance, risk, and compliance (GRC) programs can be well worth the investment. Technology plays an integral role in the success of such programs by providing much-needed consistency, efficiency, and insight. But as software vendors target the growing GRC market, it becomes increasingly difficult to distinguish what they offer. Forrester's GRC Technology Ecosystem provides a foundation for identifying how various GRC technologies fit into existing programs and the important roles they can play. See the February 3, 2009, "The GRC Technology Puzzle: Getting All The Pieces To Fit" report.

[4]    KPMG decided not to participate in this year's evaluation.

[5]    In the past, Forrester evaluated security consulting and risk consulting services in separate Waves. See the September 25, 2007, "The Forrester Wave™: Security Consulting, Q3 2007" report and see the June 25, 2007, "The Forrester Wave™: Risk Consulting Services, Q2 2007" report.

# FORRESTER®

## Making Leaders Successful Every Day

For information on hard-copy or electronic reprints, please contact Client Support
at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®