TBR

TECHNOLOGY BUSINESS RESEARCH, INC.

TBR EVENT PERSPECTIVE

PwC relies on trusted brand, skilled talent to expand in cybersecurity

PwC Cybersecurity and Privacy Analyst Day

Miami, May 3-4, 2016

Patrick M. Heffernan (patrick.heffernan@tbri.com), Principal Analyst and Practice Manager

Stephanie Artigliere (stephanie.artigliere@tbri.com), Analyst

Event overview

On May 3 and 4 TBR returned to PwC's Experience Center in Hallandale Beach, Fla. We spoke with PwC leaders and clients in small group sessions and participated in demonstrations that allowed us to experience tools and games PwC uses with clients to identify and road map cybersecurity needs. Throughout the event PwC highlighted its talent as its core differentiator, emphasizing its cybersecurity adviser role within its clients' organizations. The PwC team stressed how firm management recognizes that every element of its business — advisory, deals, risk, audit — needs to embed cybersecurity. Differentiating its technology practice with its people and working collaboratively across its member firms to offer a global cybersecurity portfolio does not surprise us. This approach to cybersecurity mirrors what we heard in March at PwC's Digital Analyst Day, also at PwC's Experience Center, and ties to the firm's overall business transformation since the firm started rebuilding its consulting practice to work more collaboratively across its network.

Trusted brand, record of success and significant investments demonstrate PwC is serious about its cybersecurity and privacy practice

PwC employees noted that the majority of clients recognize they need to ramp up investments in cybersecurity and privacy to mitigate risks and meet compliance regulations on data privacy, but also need guidance from a cybersecurity consulting partner to plan, execute and essentially extend their cybersecurity teams. PwC has a two-decade track record of delivering security offerings, but TBR notes a substantial increase in PwC's activity in the last year, particularly around talent, technology and even marketing. All of this will continue to position PwC for opportunities around helping clients assess current cybersecurity and privacy measures, identify risks, develop strategies and execute on cybersecurity road maps. As PwC continues to invest heavily in the cybersecurity space, we expect the firm to play to its strength of expanding long-term client relationships by proactively helping these clients embed cybersecurity into their business models. During the event we heard directly from PwC clients who spoke to the firm's dedication, hands-on approach and ability to deliver on its strategy-through-execution promise. PwC's cybersecurity practice will rely on client trust, as evidenced by a chief information security officer (CISO) who

spoke about switching organizations and bringing PwC with her as an extension of her team. As the company implements cybersecurity solutions into its business and offers similar solutions to its clients, we expect PwC will promote its own proofs of concept, which, combined with maintaining its transparent pricing model and ensuring clients know the firm's scale and capabilities to quickly assemble a team to respond to a cybersecurity attack, will build the firm's reputation as a trusted cybersecurity partner. We anticipate PwC will trial new offerings with willing long-term clients and highlight client success stories over time, attracting new clients through its cybersecurity and privacy portfolio. While cybersecurity remains a top concern of the C-Suite and PwC's permission to play will give the firm an advantage over competitors, we believe PwC faces steep competition in this space from vendors with technology-heavy portfolios, SIs and public sector vendors with well-established brands in cybersecurity.

People and tools bolster PwC's role as a cybersecurity partner

We heard how PwC leaders recognize the challenge of finding cybersecurity talent and how over the past year the firm introduced a cybersecurity boot camp, revamped its training program and developed career paths that help attract and incent employees to remain loyal to PwC. These investments span onshore and offshore locations, allow employees to choose where they would like to specialize and help PwC build technical expertise. PwC's current cybersecurity practice boasts more than 2,700 people ranging from regulatory experts, CISOs, lawyers, data scientists and consultants. We expect the firm to continue to acquire, making purchases similar to Praxism; however, due to the competitive cybersecurity market, an organic approach will remain at the forefront of PwC's talent expansion strategy.

To augment its cybersecurity and privacy expertise PwC develops tools, leverages partners and offers managed services, enabling the firm to move beyond the strategy stage to implement solutions and cultivate longer-term client relationships. At the event we experienced tools and games (e.g., Cybersecurity Assessment Tool and Game of Threats) the firm uses with clients to assess the current state of their business, develop road maps and walk through virtual cyberattack scenarios that help clients identify what they need for protection and develop incident response-readiness plans. To fill portfolio gaps PwC leverages partners from emerging to established multibillion-dollar organizations. While the firm jointly develops cybersecurity offerings with technology vendors such as Google, PwC leaders spoke to the firm's vendor-agnostic approach, which feeds its consulting-led model and role as a cybersecurity partner to clients. PwC recently branched out beyond its traditional services by offering cybersecurity managed services and a threat protection platform "as a Service." The implementation and operations leaders stressed how PwC differentiates its managed services by tying in project work and experts to help clients best gain and use information from managed services after they are deployed. These somewhat nontraditional service offerings for the firm enable it to maintain longer services contracts on a subscription basis and will help PwC build its reputation beyond a consultancy. While PwC has added SaaS and managed services to its offerings, a definite expansion beyond the firm's traditional business model, TBR does not anticipate these specific offerings will become a broader trend throughout PwC.

TBR perspective

Even though PwC integrated its cybersecurity and privacy practice across its global member firms, leverages people as its core asset to maintain its trusted adviser role and expands into nontraditional service offerings, the firm faces an uphill battle against fierce competition. We believe PwC's move to build a substantial cybersecurity practice strengthens its role to advise around digital transformation and ability to cross-sell and upsell its portfolio offerings as cybersecurity naturally adds to the firm's business and industry strategy, risk and compliance expertise. By offering "as a Service" solutions PwC will deliver on its strategy-through-execution promise and capture more revenue over time by signing longer sales contracts likely composed of strategy initially, then moving into managed services with a "white glove" service. PwC leaders noted 40% of cybersecurity leads stem from technology partners, so while the firm increasingly develops offerings outside of its traditional services, maintaining its cybersecurity ecosystem and vendor-agnostic approach remains part of its strategy.

Through the rest of 2016 TBR will watch for the following stemming from PwC's Cybersecurity and Privacy practice:

- Scale cybersecurity talent — Continued investment in training and offering of career paths is crucial for PwC to retain talent and scale its expertise to deliver on its promises to quickly gather the team to support clients in incident response mode and deliver "white glove" service in implementation and operations.

- Record of success stories and use cases of leveraging the Experience Centers — PwC will attract new clients, expand addressable market, build its reputation as a cybersecurity partner and win larger contracts by embedding cybersecurity offerings into digital transformation engagements and using itself as a proof of concept.

- Collaboration — While TBR believes PwC works more collaboratively across its network of member firms, relative to some of its Big Four peers, we'll look for how PwC shares and applies frameworks and best practices across geographies and industries where appropriate.

- Acquisitions — Big Four peers and SI vendors leverage acquisitions to aggressively scale cybersecurity expertise and IP. We will watch closely to see if PwC keeps pace with competitors or mainly sticks to its organic approach.

- Joint business relationships — Throughout the event PwC did not weigh one joint business relationship over another, signaling its intent to play as a vendor-agnostic consultancy and best meet the needs of clients on a case-by-case basis. TBR will examine whether PwC tightens its relationship with a particular technology vendor in the cybersecurity space, such as the firm's move to work closely with Google to expand its cloud capabilities.

- Performance — We will look to see if PwC reports its cybersecurity practice continues to grow at more than 25% per year.

Technology Business Research, Inc. is a leading independent technology market research and consulting firm specializing in the business and financial analyses of hardware, software, professional services, and telecom vendors and operators. Serving a global clientele, TBR provides timely and actionable market research and business intelligence in a format that is uniquely tailored to clients' needs. Our analysts are available to address client-specific issues further or information needs on an inquiry or proprietary consulting basis.

TBR has been empowering corporate decision makers since 1996. For more information please visit www.tbri.com.