TBR

TECHNOLOGY BUSINESS RESEARCH, INC.

TBR EVENT PERSPECTIVE

Understand, Be, See, Expel: Security on the cusp of disruption

Accenture Security: Analyst Summit 2017

Bangalore, India; April 19-20, 2017

Authors:

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

Bozhidar Hristov (bozhidar.hristov@tbri.com), Senior Analyst

Understand the threat. Be the threat. See the threat. Expel the threat. A company that can provide all those things to clients is a true end-to-end cybersecurity services vendor, capable of serving clients and disrupting the market with offerings and capabilities that will force competitors to invest, align, merge or leave the market.

TBR perspective

Accenture Security made a splash in 2015 when it acquired FusionX, following Accenture's pattern of acquiring leading-edge talent but potentially harnessing a new kind of security services offering to Accenture's existing global scale. Eighteen months later, the firm found its footing with high-functioning security operations centers (SOCs), innovation R&D labs and tightly run managed security services offerings, in some locations blended into Cyber Fusion Centers. If Accenture has been slow to fully develop its offerings and quiet about the depth and scale of its security operations, that will likely change in 2017 as the market begins to appreciate Accenture's new mission and capabilities.

Event overview

On April 20 Accenture Security hosted six analysts for a full day at the Bangalore, India, Cyber Fusion Center, affectionately known as "Bang 9." In addition to presentations and an extensive Q&A session with Accenture executives, the center's staff detailed operations across managed security services, a state-of-the-art security operations center, client-dedicated war rooms and innovation/hacker labs.

Industry-centric and locally supported services: not new, but at scale

Reflecting Accenture's industry-centric DNA, Accenture Security executives at the event frequently talked about understanding the core characteristics of a client's industry before trying to develop a cybersecurity solution. For example, as they work in an industry with a strong safety-first culture, oil and gas security professionals

understand an approach that highlights how IT vulnerabilities could lead to physical accidents and deaths. Similarly, financial services clients understand risk more than most and appreciate a cybersecurity discussion framed around risk concepts. While not unique, this approach plays to Accenture's overall strengths and should help the firm more rapidly sell and scale. Overall, Accenture Security executives said their approach centered on addressing the business risks of a security incident before the technology risk.

As part of a live table-top exercise, Accenture Security leadership described different client-specific engagements throughout the day, highlighting a reliance on locally deployable or regionally based resources. The SOCs serving global clients and the fused capabilities in Bangalore and elsewhere still depend on local assets deployed to client sites to ensure results. This element reflects an overall trend at Accenture — to become more locally grounded, even as the firm keeps its global delivery network in place — and among professional services vendors more broadly, with better management of local and regional resources driven by both client demand and consultants' emerging work-life expectations (see TBR's *Management Consulting Benchmark* to be published in May).

Revenue-driven strategy backed by partners' technologies, delivery network and application services position Accenture to disrupt the MSS market

Over the past 18 months, Accenture bolstered its security services capabilities and scale through both acquisitions and industry hires. Completing eight acquisitions and minority investments enabled Accenture to gain access to over 800 cybersecurity professionals with skills in cyber defense, digital identity and access management, application security, and managed security services (MSS).

While the purchases of Defense Point Security and Endgame's federal government services business will further support Accenture Federal Services' proactive cyber defense capabilities, iDefense, which has been rapidly integrated, has begun to act as the backbone of Accenture's MSS capabilities, augmenting Accenture Cybersecurity Engine offerings around threat intelligence and monitoring. MSS are delivered by security-trained personnel within Accenture's network of Cyber Fusion Centers across the globe through a multitenant shared services model. Centers are staffed with L1 through L3 analysts, whose individual experience ranges from three to more than seven years, and divided into clusters, with each cluster serving two or three clients, depending on the number of client devices that need to be managed. The Cyber Fusion Centers offer 24/7 response services supporting both chief information security officer (CISO) and COO functions across the value chain. Additionally, alliance partners play a pivotal role in Accenture's MSS offerings. Through its four-way partnership with Splunk, Palo Alto Networks and Tanium, Accenture is integrating endpoint threat visibility (from Tanium), network threat visibility and control (from Palo Alto Networks), and a correlation engine (from Splunk) to secure the three main technologies Accenture needs to implement a basic threat detection and, to a lesser extent, response strategy. While Accenture is creating a tactical solution rather than a strategic one, if the offering is priced properly, the company will be able to more easily deliver threat detection and response that is run through its managed services facilities globally. Additionally, Accenture's revenue-driven strategy paired with company's investments in innovative technologies, especially around automation, can help catapult Accenture's MSS performance, particularly as clients seek to optimize opex structures through adoption of less-labor-intensive products.

Managing a network of SOCs and offering a wide array of services from monitored or managed intrusion detection systems through distributed-denial-of-service protection sum up what a legacy MSS vendor looks like, with services primarily geared toward infrastructure management and monitoring. We see Accenture's approach to security as a business risk rather than a technology risk, and the company's application services prowess will help it disrupt the legacy MSS market and create a new category addressing security pain points outside the CISO office around application security, assurance, and governance and risk. To build scale in the MSS space, Accenture is developing a threat intelligence strategy around the convergence of IT and operational technology by using threat analysis and by leveraging custom sensors and/or heavily using robotic process automation-based tools based on partner-run IP such as Blue Prism.

No time for digital transformation when you are on a mission

Beyond the technology details, two elements struck TBR as noteworthy: a sense of mission and a lack of hype around digital transformation. Of the first, Accenture Security's leadership repeatedly spoke of the cybersecurity landscape as a broken, chaotic and poorly served ecosystem, in which too many vendors provide small and insufficient patches to major problems. While not quite rearranging the deck chairs on the Titanic, Accenture's overall philosophy appeared to be that massive vulnerabilities could only be addressed with market-disrupting changes brought about by the largest and most influential players — something Accenture intends to become. In one case, Accenture Security executives described how the firm's long-standing dedication to Global 2000 companies would have to be worked around to address cybersecurity weaknesses at a smaller enterprise level — weaknesses that endanger an entire industry. Accenture Security does not have an explicit mission to disrupt Accenture, but clearly believes its mission extends beyond simply providing security services to its clients.

Second, one phrase never surfaced during the entire event, including the opening and closing receptions and dinners: "digital transformation." TBR's developing understanding of digital transformation includes cybersecurity services as a foundational component, a necessary element of anything digital. Perhaps reflecting their practical realism (possibly brought about by being later to the market), Accenture's executives skipped the buzzwords and spoke only at length about actual implementations and engagements, as well as innovations on the cusp of pilot projects. Understanding that practitioners engaging in a deep dive into their specialty will typically avoid marketing hype, TBR was still surprised the larger, relentless professional services buzz around digital transformation had not crept into Accenture Security's efforts to showcase for analysts their current work and expectations for the next few years.

An operations order for Accenture: invest, disrupt, simplify, grow

TBR will continue to track closely how Accenture Security evolves, both in the marketplace and in terms of the business group's performance. TBR sees four defining approaches in early 2017: 1) investment in R&D that will produce quickly tangible results (e.g., robotic process automation), fueling disruption; 2) a mission to disrupt security (for the better for all companies in all industries, Accenture client or not); 3) a practical, no-hype, minimal-marketing approach to operations and delivery; and 4) expectations for revenue growth outpacing headcount growth, even as new centers open and service offerings expand into new areas. By assessing changes to those approaches over 2017, TBR will develop a deeper understanding of Accenture's likely expanding position in the security services market.
