Market Insight Report Reprint

With consulting services, AT&T aims to help enterprises rethink their approach to cybersecurity

June 8 2021

by Aaron Sherrill

The company is helping enterprises reframe how they think about cybersecurity with a portfolio of professional and consulting services focused on enabling organizations to achieve operational objectives, improve their cybersecurity posture, address digital transformation initiatives and drive business outcomes.

451 Research

S&P Global
Market Intelligence

Introduction

Despite an abundance of successful cyberattacks on organizations of every size and industry, many companies remain unprepared. However, enterprises are beginning to recognize that organizational resilience requires a fundamental change of mindset, requiring them to consider cybersecurity as a strategic priority rather than an operational issue. AT&T aims to help enterprises reframe how they think about cybersecurity with a portfolio of professional and consulting services focused on enabling organizations to achieve operational objectives, improve their cybersecurity posture, address digital transformation initiatives and drive business outcomes.

THE 451 TAKE

Cybersecurity consulting services are shifting away from single, monolithic projects toward a blend of recurring services that encompass strategic consulting, guidance and implementation services along with ongoing managed service engagements. Organizations are looking to maximize the value of their partners; many prefer to engage providers that can deliver a broad range of services that can be tailored to their specific needs. With their global presence, expansive network and connectivity, broad customer base, and long history of managing and delivering cybersecurity at scale, telcos like AT&T are particularly well-positioned to help customers tackle a broad range of cybersecurity challenges and securely harness the power of new technologies such as 5G, IoT, AI and the cloud.

Context

Founded more than 140 years ago as the Bell Telephone Company, AT&T is well known for its global communications network. Over the years, the company has expanded its portfolio to include services that span networks, IoT, mobility, voice and collaboration, cloud, and cybersecurity. In 2019, AT&T announced AT&T Cybersecurity, which combines the technology and threat intelligence from its acquisition of Alien Vault and the company's security consulting and managed services. Although the AT&T Cybersecurity nomenclature may still be relatively new to many in the market, the company has been delivering cybersecurity services for over 25 years.

The company maintains eight global security operations centers (SOC) and employs over 2,000 cybersecurity specialists who have an average of 12 years of experience. Managed security services have been an area of strategic expansion for AT&T Cybersecurity; however, consulting services remain a key ingredient to meeting customer needs.

Delivering services that span security strategy and operations; risk strategy, compliance, privacy and data governance needs; and vulnerability management and incident response, AT&T is helping customers strengthen their cybersecurity posture and increase their cyber resiliency by enabling organizations to align cyber risks to business goals, meet compliance and regulatory demands, achieve business outcomes, and be prepared to protect an ever evolving IT ecosystem.

Consulting services

Although most enterprises are still struggling with the challenges of cybersecurity, AT&T says it has seen a shift occur over the last decade, with organizations now viewing security in terms of risk and the ability to achieve business outcomes rather than just a necessity to meet compliance requirements. This shift has happened across verticals, geographies and businesses of every size. The company says this shift has spurred deeper conversations with customers that go beyond just addressing the technology challenges of cybersecurity and beyond conversations limited to CIOs or CISOs. Business stakeholders and other decision-makers are increasingly asking critical security questions that impact their digital transformation initiatives, product lines, divisions, customers, partners and employees. They are also increasingly interested in how cybersecurity can reduce costs, be used as a competitive differentiator and increase revenue performance.

In response to the shifting view of cybersecurity, AT&T has organized its cybersecurity consulting services around three pillars: risk advisory services, cyber operations and cyber as a service (CaaS); each encompasses a variety of services designed to help organizations tackle an assortment of cybersecurity challenges.

Risk Advisory Services. AT&T's Risk Advisory Services help organizations evaluate and improve existing security governance by considering business challenges, requirements and objectives. This group helps organizations build strategies and plan roadmaps; address data privacy, third-party risks, fraud and payment security challenges; and contend with IT regulatory compliance needs and gaps.

As AT&T has helped customers build out cybersecurity strategies and roadmaps, it has found that organizations are shifting away from traditional three-to-five-year plans, preferring to develop 18-to-24-month plans and strategies. The speed of business, the rapid adoption of new and emerging technology, and the ever-evolving threat landscape are pushing organizations to become agile and flexible in building their plans. The company says organizations are also becoming more strategic in their investments, seeking to make data-informed decisions to better prioritize and align to business initiatives and ensure that investments achieve the outcomes desired and offer a justifiable return on investment.

Cyber Operation Services. Focused on technical solutions that enable organizations to achieve operational objectives and drive business outcomes, AT&T's Cyber Operation Services span network and cloud security, application security, mobile, IoT and endpoint security, and threat detection and response services. The company says its cyber operation services are designed to address both the traditional security challenges that have been plaguing enterprises for the last decade and the security issues that come with digital transformation, helping enterprises prepare for future security challenges. Positioned to support organizations in developing or enhancing cybersecurity operation through technology implementation and improving defenses and response across endpoints, networks, clouds and applications, AT&T says it can deliver customized services that span staff augmentation and SOC design and implementation, as well as address challenges in IT, OT and IoT environments.

Cyber as a Service. AT&T's CaaS portfolio offers subscription-based services designed to support the ongoing, day-to-day resilience needs of cybersecurity programs. Spanning vulnerability management, incident response and forensics, risk and compliance management, and training and awareness services, CaaS provides proactive, ongoing and reactive services that enable organizations to consume services and skill sets on demand based on business needs.

Competition

Rapidly changing market dynamics are creating pressures for cybersecurity consulting providers to continuously stay ahead of the curve with new service capabilities and delivery models. At the same time, providers must develop talent and expertise to deliver services that span traditional security needs and gaps as well as emerging technologies, including SASE, zero trust, AI/ML, 5G, automation and analytics.

Overall, the market for delivering cybersecurity consulting capabilities is highly fragmented, with services offered by providers ranging from global technology and security firms to local and regional MSPs in addition to technology vendors. AT&T faces competition from firms like Deloitte, IBM, EY, Accenture, KPMG, Booz Allen Hamilton, Atos and PwC. It also competes with other traditional telecommunication firms that have expanded into cybersecurity services, including Verizon, Lumen (formally CenturyLink), Vodafone, BT, Telefonica and Orange.

MSPs such as One Neck, All Covered, Netgain Technologies and Six Degrees, as well as MSSPs such as Avertium, the Herjavec Group, TrustWave, Secureworks and Cipher compete with AT&T on many fronts in the cybersecurity market.

SWOT Analysis

STRENGTHS

AT&T's strong credentials, global network and long history of managing and delivering cybersecurity at scale provide the company with unique advantages that can be difficult for most competitors to duplicate. AT&T's broad portfolio of cybersecurity offerings that span consulting services, managed services and technologies enable the company to help customers at any point along their security maturity journey.

WEAKNESSES

Competition in the security services space is fierce, with a wide variety of firms offering consulting services. While many organizations are aware that AT&T offers cybersecurity services, the company will need to promote the breadth and depth of its cybersecurity capabilities to a broader market. The company will also need to target both security professionals and other decision-makers within organizations that are recognizing the value of cybersecurity within their domain of influence.

OPPORTUNITIES

Organizations of every size and industry are looking for help improving their cybersecurity posture. However, small and midsized organizations tend to have a longer security maturity journey ahead of them. Partnering with MSPs that have already established themselves as a trusted advisor to their customer base could be a force multiplier for AT&T while enabling MSPs to deliver greater value to their customers with advanced security consulting services.

THREATS

Keeping pace with continuous technology innovation and the evolving attacks that target an ever-expanding digital footprint is a challenge for any organization but is amplified for security service providers. AT&T will need to continue to evolve its security service capabilities to meet these challenges, along with changing regulatory demands, customer demands and expectations, and increasingly complex customer IT ecosystems.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence