AVASANT

CYBERSECURITY

FROM REACTIVE DEFENSE TO PROACTIVE DIGITAL ENABLEMENT

As enterprises transition to cloud and integrate digital technologies to generate new revenue streams, there is no longer a secure perimeter and the data-centric security strategy has become critical.

Cyber threats are amplified as enterprises in their quest to digital transformation adopt next-gen technologies to re-define their business model and accelerate their time to market. Though Cloud, IoT and Mobility are digital enablers, they have also widened the risk perimeter beyond organization networks, giving rise to opportunities for a new breed of "smart" attacks.

As enterprises re-define their security strategy and align it per emerging threat landscape, their dependency on providers for specialized cybersecurity needs has increased. To address this rising demand and remain competitive service providers need to invest in talent development, enhancing organization structures and expanding partner network to strengthen their security portfolio.

CYBERSECURITY - FROM REACTIVE DEFENSE TO PROACTIVE DIGITAL ENABLEMENT

Owing to sudden spread of ransomware, well planned advanced persistent threats and data integrity attacks and the swift growth in coin miners, the nature of cyber-attacks has increasingly become more varied and sophisticated in nature.

Such cyber threats are further amplified as enterprises in their quest to digital transformation adopt next-gen technologies to re-define their business model and accelerate their time to market. Though Cloud, IoT and Mobility are digital enablers, they have also widened the risk perimeter beyond organization networks, giving rise to opportunities for a new breed of "smart" attacks.

Having said that, the enterprises still need to address older threats and continuing challenges as malicious email and spam continue to be the key tools for hackers to distribute malware as they take threats directly to the endpoint. The Pennsylvania Department of Education breach in February 2019 highlight the incidents linked to human error continue to persist which account for more than 80 percent breaches.

Though enterprises are aware of these threats, progress to a proactive approach is still slow. For cybersecurity to be effective, the enterprises must adopt a dynamic posture towards cyber threats and apply progressive thinking to make its process, people, and technology secure:

- **Process:** It's imperative for enterprises to have an independent second line of defense (Enterprise Risk Management team) that reviews and checks the first line (Core Information Security team) and involve financial controller and Human Resources for effective security posture.

Core Information Security	Enterprise Risk Management	Internal Audit
1st line of defense	2nd line of defense	3rd line of defense
Primarily responsible for managing its own process. Identify and control risks through patching, ID Administration and adequate controls.	Independently review and report into management board / CXOs. Involves financial controller and HR for effective security posture.	Assure design and effectiveness of 1st and 2nd line of defense. Reports into management and audit committee.

Additionally, it is crucial for an enterprise to build an effective, resilient third-party risk management function to mitigate risks from one of the biggest known sources of incidents - more than 25 percent increase is witnessed in the average cost of third-party breaches.

Hence, both sourcing criteria and contract terms while engaging with outsourcers need to change to reflect this threat. Elements such as "Right to Audit" clauses become critical in any MSA and service contract.

- **People:** It is essential to build the right Information Security (IS) staff, to ensure basics such as adherence to patching and identity policies. Enterprises are deploying three-pronged strategy to achieve this:
    1. Partner with cybersecurity companies to tap talent,
    2. Leverage digital technologies for virtual trainings and in-house talent development programs, and
    3. Host hackathons to spot right talent at half the cost and time of traditional ways of hiring.

- **Technology:** Digitalization has stirred up the demand for advanced techniques, such as cyber-attack simulations and automated threat detection, to identify security risks. Additionally, the increased regulations and use of IoT devices have driven the demand for cyber forensics.

As the threat environment becomes more complicated and advanced, the enterprise reliance on service providers for specialized cybersecurity needs increases. To address this rising demand, the service providers are developing new roles such as Threat Hunter, IoT and OT Security Architect / Consultant etc. and in parallel incubating talent in partnership with education institutes. For instance, Fujitsu partnered with University Technical Colleges (UTCs) across England with a goal to train 500 students a year in cybersecurity skills. Whereas, Accenture invested USD 500K in the Georgia Institute of Technology's online master's degree program in cybersecurity that lets students apply technical knowledge in a business context for the utility sector.

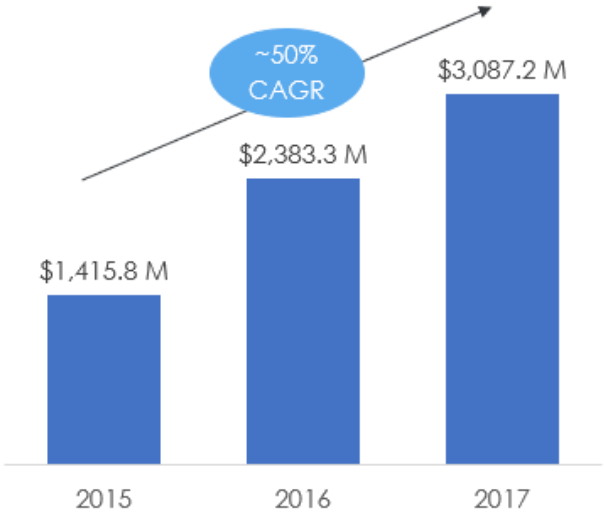
Additionally, to remain competitive, service providers continue to acquire cybersecurity companies to enhance their security capabilities and expand their geo reach. The latest in the series was Capgemini acquiring Leidos Cyber to strengthen its cybersecurity services in North America. Another popular one was AT&T acquiring threat intelligence company, AlienVault, to help expand its security offerings for enterprises to smaller businesses.

For the way forward, enterprises should continue to shift from network-centric security toward data-centric security strategy as the reliance on data becomes pivotal across three levers of an enterprise: employees, third parties and suppliers. Additionally, owing to the use of cloud

services and mobile workforce, this shift becomes even more evident as the secure perimeter increasingly expands.

Secondly, the CISOs role will continue to advance and become more and more critical from business enablement standpoint. And, as GDPR evolves and more similar regulations emerge across North America, CISO's role will be vital to formulate and continually improvise existing compliance related protocols. Hence, for progressive enterprises it's imperative to involve CISOs at the beginning of business project cycle to ensure secure launch, hence mitigate reputation damage and financial loss.

Thirdly, cyber insurance, a key lever to risk management across industries is on the rise owing to the increase in number of cyber data breaches and the transition to cloud-based services.



In fact, between 2015-17, the total cyber premium written have increased around 50%. It is expected to hit USD 10B in next 3 to 5 years as enterprises are shifting focus from short-term cyber insurance policies to addressing the more important aspect of maintaining long-term reputation with stakeholders.

About Avasant Cybersecurity Services Radarview™

Avasant Cybersecurity Services RadarView™ report covers the top 28 service providers that have shown mature capabilities, future-aligned investments and innovations, and consistent growth in their Cybersecurity offerings. The report recognizes the top service providers as follows:

- Leaders: Accenture, AT&T, HCL, IBM, Secureworks, Symantec, Trustwave, Wipro
- Innovators: Atos | Syntel, British Telecom, DXC, Fujitsu, NTT Security, TCS, Telefonica
- Disruptors: Capgemini, CenturyLink, Cognizant, Infosys, Orange Business Services, Tech Mahindra, Verizon
- Challengers: CGI, LTI, Mphasis, T-Systems, UST Global, Zensar

Download Avasant's complimentary 89-page report here.

About Avasant

Avasant is a leading management consulting firm focused on translating the power of technology into realizable business strategies. Specializing in digital and IT transformation, sourcing advisory, global strategy, and governance services, Avasant prides itself on delivering high -value engagements through industry focused innovation and flexible client based solutions.

Email – contactus@avasant.com | Phone - +1 310 643 3030 | Visit us at - www.avasant.com