CyberProof Wants to Disrupt the Managed Security Services Market

By Stanton Jones, Antoine Viale

Briefing Note

Reprint

March 2020

Reprinted courtesy of

UST Global®

ISG Research™

Contents

About ISG Research™

ISG Research™ provides proprietary research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ gives business and technology leaders the insight and guidance they need to accelerate growth and create more value.

For more information, please email **contact@isg-one.com**, call +1.203.454.3900, or visit **research.isg-one.com.**

SUMMARY & KEY INSIGHT

The World Economic Forum **ranks cyberattacks** as the second most concerning risk for businesses globally over the next 10 years. And rightly so. Organizations are **one-third more likely** to experience a breach in the next two years than they were in 2014. And costs associated with breaches are increasing. In 2019, the **average total cost** of a data breach was nearly four million USD, primarily due to a reduction in business based on loss of customer trust. Attitudes inside companies are changing as well. We see cybersecurity rapidly evolving into a board-level discussion. Given the inevitability of a breach, corporate leaders are demanding that management define risk tolerance levels and put plans into place that ensure risk stay within these levels.

This presents a challenge for enterprises. To effectively defend against a rapidly changing threat landscape, companies need technology, expertise and threat-based intelligence, at scale, which explains the growing demand for third-party security services, specifically managed security service providers (MSSP). CyberProof, a UST Global Company, has developed a compelling MSS offering that addresses these three components, delivered via an outcome-based commercial model that translates to the kinds of outcomes boards expect. Companies in banking, insurance, healthcare and travel/ transportation should consider shortlisting CyberProof to meet this rapidly evolving demand from board members, management and customers.

PERSPECTIVE

We were recently briefed by CyberProof, a UST Global Company. Parent company UST, which was established in 1999, is a well-known provider in the IT services industry. UST has over 25,000 employees and more than 140 Global 1,000 clients, many of whom have been with UST for well over a decade.

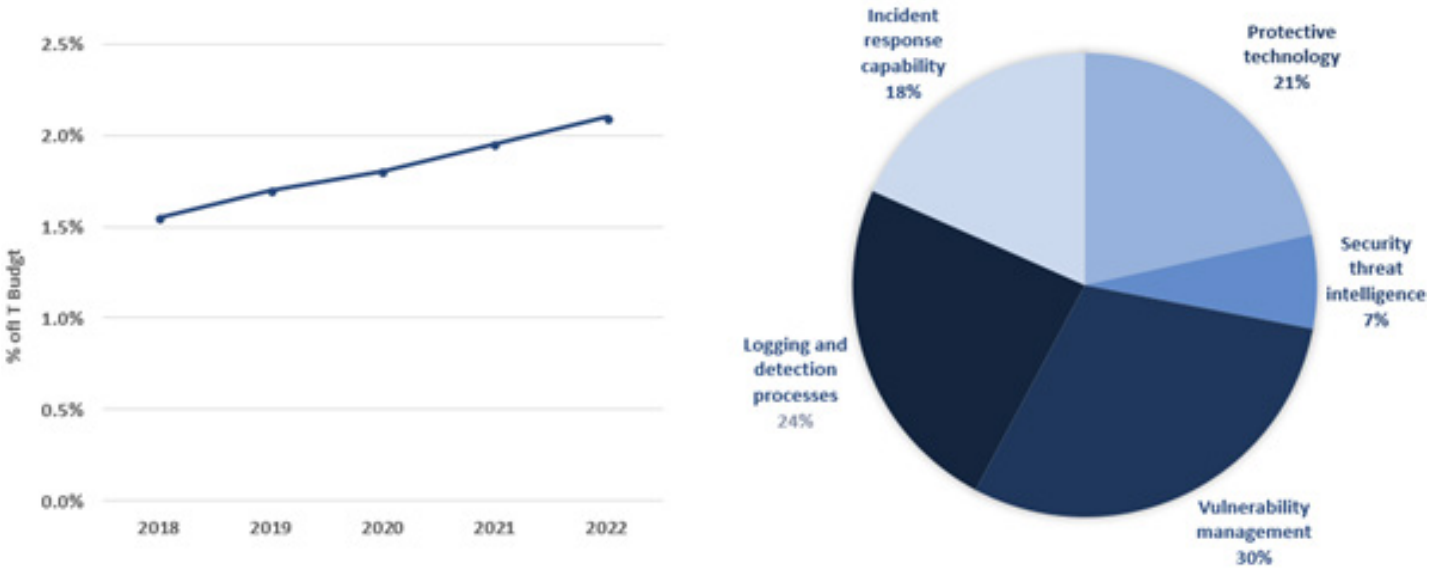
CyberProof is based out of Tel Aviv and was created as a new company to tap into the fast-growing start-up ecosystem in Israel. Israel has become a hotbed of cybersecurity innovation. In 2019, Israeli startups **received 20 percent** of the global venture capital investments in cybersecurity. Israeli security firms have also become known for tackling some of the industry's toughest problems – challenges more traditional firms often avoid. It's this "no problem too hard" spirit that CyberProof appears to want to emulate.

CyberProof positions its offering as "next generation managed security services" based on the idea that it can perform hygiene-related security services and other services, such as threat hunting and behavioural analytics. CyberProof delivers these services in a c-o-delivery model by supplementing an enterprise's existing security services. ISG sees many clients preferring this model, having realized that over the past twenty years outsourcing security architecture and planning has hamstrung them. CyberProof's co-delivery model supplements an existing staff, solving the three major problems discussed before: technology, skills and access to data.

While all leading MSSPs have an impressive array of technology and talent, it is CyberProof's case study with a large financial services company that we feel differentiates it in the MSSP space. The arrangement is a combination of cloud-based technology, an operational model that puts CyberProof resources alongside customer resources, and a pay-per-device commercial model that encourages both sides to reduce risk over time.

We feel this is especially important to banking and financial services companies given the significant increase in IT spend on security services over the next two years (**Figure 1**). In 2019, the recurring costs of a Security Operations Center (SOC) in the financial industry vary from 1.4 percent to 1.7 percent of the entire IT budget. ISG expects that, by 2022, the SOC costs will exceed 2 percent of the IT budget due to increasingly stringent regulatory requirements.

Figure 1: Distribution and Percentage of IT Budget for Security Services in BFSI: 2018-2022



Source: ISG Research

REFERENCES

In the case of the large financial services company, here's what differentiated CyberProof's MSSP offering:

Cloud-native technology stack: CyberProof uses Microsoft Azure Sentinel as its preferred security information and event management (SIEM) system. Leading SIEM systems perform data collection, anomaly detection, threat hunting and orchestration. What is interesting in this case is the degree to which CyberProof is "all in" on its relationship with Microsoft. In a recent meeting between the two, Microsoft indicated it is impressed with how CyberProof is using its SIEM to help customers. For Microsoft-centric clients, this tight partner relationship could be a plus. CyberProof does support other SIEM systems such as Splunk and IBM QRadar.

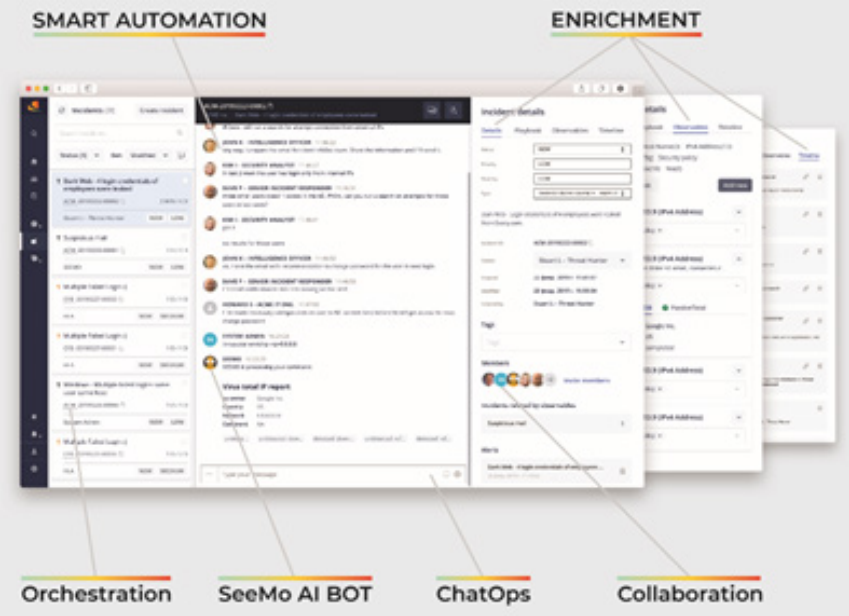
Hybrid staffing model: CyberProof uses a co-delivery model, which means it becomes an extension of the customer's team. CyberProof makes it clear it is not interested in a traditional outsourcing model in which existing customer staff transfer to the provider. Early indications from this financial services customer (which is in transition now) indicates it is happy with results so far, with feedback that CyberProof is a good cultural fit, focused on the client and able to respond quickly to change.

Use-case factory: CyberProof has adopted an Agile approach to operations whereby it defines threat use cases, adds them to a backlog, and then works in prioritized order using sprints. Essentially, the new security team works like a product team, using a combination of CyberProof and customer resources, both offshore and co-located.

Autonomous correlation, enrichment and alerting: CyberProof has developed a virtual analyst dubbed "SeeMo." Like other virtual analyst technologies, it uses a combination of narrow artificial intelligence (AI) techniques, such as natural language processing, to automate knowledge work. CyberProof believes SeeMo will eventually perform 70 percent of the work a security analyst performs, and when it does, CyberProof will be able to pass on the resulting savings to current and prospective customers. While the virtual analyst technology is not unique, applying it in this way – specifically around enrichment of data so humans can do their jobs faster – appears to be particularly mature compared to competitors.

Commercial Model: CyberProof offers a unique commercial model. The financial services customer claims that CyberProof had the best marginal costs to absorb volume growth. It can do this because it offers its service on a Resource Unit basis. This means the client is paying for what it uses or what it creates: use cases, deception assets, devices, etc. This is a differentiation for CyberProof as enterprise clients are purchasing hardware, software and managed services – creating a jumble of fixed and variable, operational and capital expenditures – with little ability to define outcomes (in this case, risk reduction) for the investment.

Figure 2: CyberProof SeeMo Virtual Agent Integrated into Operations



Source: CyberProof, a UST Global Company

Focus on research: Given the risk profile of enterprises is getting exponentially larger and more complex, CyberProof understands that MSSPs need better and faster ways to sense and prevent attacks. To this end, CyberProof is funding academic research with institutions like MIT, Stanford, and Cambridge, and is participating in government-funded initiatives like the Center for Cybersecurity Analytics and Automation (CCA). By investing in cyber security ecosystems and algorithms, CyberProof can validate and test the accuracy of its automation capabilities. This research then feeds into SeeMo, which creates more tactics for sensing, preventing and / or mitigating attacks. CyberProof is punching above its weight in this category, as most providers doing this kind of work are larger.

GUIDANCE

According to Verizon's most recent data breach report, "the time from the attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes. Conversely, the time to discovery is more likely to be months." The nature of cyberattacks is changing as well. Increasingly, breaches are coming from internal actors, and are most often due to mistakes, not because of malicious intent. Case in point: Social engineering attacks are up 18 percent since 2013, and misconfiguration as a root cause of a breach is up 21 percent over the same time period.

Complexity, technical debt and lack of speed are significant enterprise challenges. But hiring more cybersecurity analysts may not be the solution. An estimated 3.5 million cybersecurity jobs will be available but unfilled by 2021. There just are not enough cybersecurity experts to meet demand. And even if there were, they can't move fast enough to meet today's threats.

CyberProof is proving it may be able to help ISG clients address these challenges and reduce cyber risk over time. We're especially encouraged to see CyberProof's long-term focus on measuring, reducing and communicating in terms of "reducing risk," rather than in terms of "increasing security." This means creating a cyber risk language that enterprise board members can understand and that addresses these common enterprise questions:

- Given our industry and geography, which attacks are we most susceptible to?
- How quickly can we detect and respond to an attack?
- What is our response window for an acceptable loss?
- How do ensure we have the right detection and response algorithms to guarantee we stay within this response window?

ISG clients should be aware that this change in thinking – and the resulting outcomes – will not happen overnight. While due diligence and effective governance is required to ensure providers meet their contractual commitments, an operating model change is also required. This means changing the way you work. Cyber security may not work best as a traditional outsourcing agreement in which the work is "thrown over the fence" to the provider. Today's threat landscape may require a client-provider partnership with each party working together in an Agile, product-aligned way to reduce risk over time. If a product-aligned operating model is new for you and your company, consider allocating the time and leadership necessary to make a relationship like this yield the desired results and reduce risk for an increasingly risk-prone world.

SUMMARY FACTS

HQ: Tel Aviv, Israel

Security portfolio: Event Monitoring, Managed Response, Use Case Engineering, Security Operations Center Services, Targeted Threat Intelligence, Breach and Attack Simulations, Endpoint Detection and Response, Vulnerability Management

Industry groups: Banking, Insurance, Healthcare, Travel and Transportation

ISG Research™
CyberProof Wants to Disrupt the Managed Security Services Market

March 2020

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

www.isg-one.com