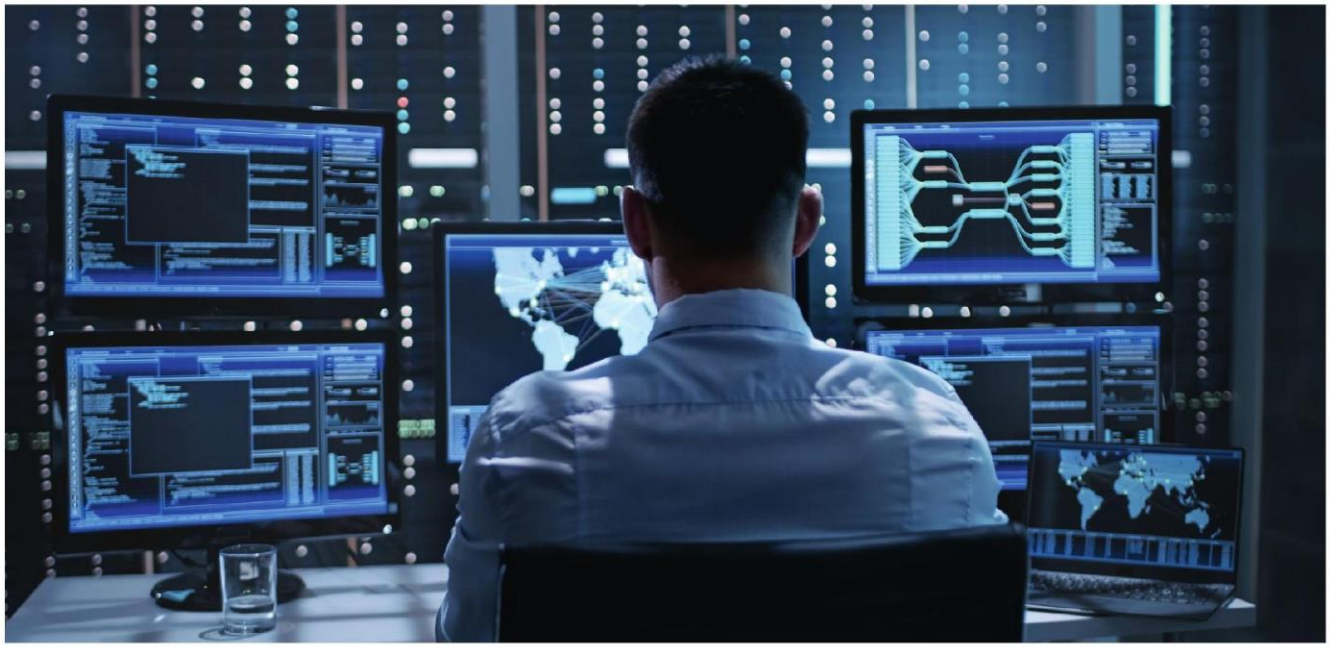

MANAGED SECURITY PRACTICE

As managed security services (MSS) start to gain wider appeal in the Middle East, the enterprise sector is offering solution providers significant integrated security solutions and growth opportunities. But what are the opportunities for channel partners that want to build a managed security services practice?

As organisations are increasing turning to managed security services providers (MSSPs) to alleviate the daily pressures they face related to information security, such as targeted malware, customer data theft, skills shortages and resource constraints, opportunities are emerging for those resellers involved in the solutions selling game.

Analyst IDC said the recent "WannaCry" worm/ransomware outbreak that infected approximately 200,000 endpoints across 150 countries, highlighted the devastating and inevitable effects of ransomware. IDC said while patching systems and preaching to end users are prudent actions, those recommendations have proven ineffective over time.

"It should be obvious to anyone preaching patch and security awareness that we have hit the limits of their effectiveness. It's time to find cost-effective, scalable solutions that gain us patch independence and cover the final mile of security," said Pete Lindstrom, vice president, Security Strategies with IDC's IT Executive Programmes.

Shadi Khuffash, regional sales manager, Carriers and MSSPs at Fortinet, said from the SMB market to large enterprise customers, cyber security is becoming more costly, complex and cumbersome to deploy, manage and maintain. Khuffash said due to the high number of crippling cyberattacks such as WannaCry and Notpetya, customers across the Middle East have become more dependent on MSSPs to secure their networks. "The market outlook for MSSP business will experience continued growth as providers in this sector further capitalise on the security challenges organisations face such as growing regulatory compliance, recruitment, budget limitations and increasing cyberattacks, he said. "We see MSSPs capturing more market share by offering a wide range of customisable security solutions and ensuring they are catering to the wider market base."

Mahmoud Mounir, regional director, Securework, said recent high-profile attacks, such as WannaCry and "Petya", illustrate the tremendous might and resource that today's cyber criminals possess.

Mounir said at the enterprise level, detecting and predicting the scale of cyber threats any organisation faces is immensely challenging and simply put, organisations that are not in the business of IT security still understand very well that cyber security cannot be ignored.

"Some organisations choose to manage their own security internally. However, this can soon become problematic, as their security teams often lack the technical know-how and the bandwidth to deploy the appropriate security controls needed to deal with today's digitally savvy and extremely resourceful adversaries," he observed. "Therefore, if the risk outweighs the internal capabilities to deploy a holistic security strategy, then organisations should look at the alternatives."

According to Mounir, one way for organisa-

For example, eHosting DataFort has been in the cloud hosting and managed infrastructure market for a long time and we have seen a huge demand for managed security services over the last few years. In our case it was a natural progression towards building an MSS practice to offer our current customers, and to tap into the growing potential customer base.

YASSER ZEINELDIN, CEO, EHOSTING DATAFORT

tions to achieve cybersecurity maturity is by leveraging a managed security service provider (MSSP). "MSSPs can help organisations stay one step ahead of potential threats by customising their security infrastructure to solve complex security and compliance challenges," he added. "MSSPs offer complete managed security services that include round-the-clock monitoring of clients' IT infrastructure coupled with state-of-the-art prevention of cyberattacks and threats to business."

He pointed out that by functioning as an extension of a company's internal security operations, they close the loop on people, processes, and technology, offering 24 by 7 support from their security operations centre.

Mounir noted that the decision to move to a managed security services model is typically driven by a convergence of IT expertise limitations, resource allocation and business needs. "Building internal managed security services capabilities puts the onus on the employees to install, configure, manage and monitor security products, which is often not a realistic ask from a time and cost perspective," he said. "Therefore, outsourcing MSS to a renowned security provider makes good business sense, and typically means a fraction of the cost compared to setting up a dedicated, in-house security team. Leaning on an expert security provider also gives organisations peace of mind when it comes to adhering to relevant security regulations."

Yasser Zeineldin, CEO, eHosting DataFort, said as a start to possible investments in providing managed security services, organisations must be able to assess and analyse the opportunities to ensure greater business success.

Zeineldin said there are several sectors that are dependent on high level of security needs including government, finance, retail and many other verticals. "A service provider

The market outlook for MSSP business will experience continued growth as providers in this sector further capitalise on the security challenges organisations face such as growing regulatory compliance, recruitment, budget limitations and increasing cyberattacks.

SHADI KHUFFASH, REGIONAL SALES MANAGER, CARRIERS & MSSPS, FORTINET

One way for organisations to achieve cybersecurity maturity is by leveraging a managed security service provider (MSSP). MSSPs can help organisations stay one step ahead of potential threats by customising their security infrastructure to solve complex security and compliance challenges.

MAHMOUD MOUNIR, REGIONAL DIRECTOR, SECUREWORK

or company playing in this space will need to have a clear strategy wherein the offerings must meet the particular requirements of each business vertical," he said. "Hardware and software investments and upgrades, security skills needs and enhancements, involve heavy cost implications. Therefore, the financial investments can play a large role in defining the MSS business."

According to Gartner, the shortage of skilled cybersecurity workers will continue, proved by the zero percent unemployment rate.

Ossama Eldeeb, regional channel senior manager, Middle East, Turkey and North Africa, and acting country manager, Saudi Arabia at VMware, said in IT security in general, there is a huge skills shortage although there is a perception that security automation reduces a certain level of control and visibility. "With all the components that come with securing an organisation's infrastructure, automation and orchestration of security processes are a must or enterprises risk being

> *Clients are no longer tied to one machine, one server, one location and the corresponding IT security needs of those clients have increased accordingly. Channel partners must find a better way to manage licenses by using a billing and licensing option where you can distribute licenses across multiple customers in a more flexible manner.*
>
> **HARISH CHIB, VICE PRESIDENT, MEA, SOPHOS**

left behind," he said.

Eldeeb added that another important point to keep in mind is that often, the tools used by MSSPs are not available commercially. "This is another strong barrier to building a managed security practice that is comprehensive enough and on par with that provided by MSSPs," he said.

According to Dipak Vagadiya, security lead at systems integrator Emitac Enterprise Solutions, security operation skills are a must with next generation analytics technologies like user behaviour analytics and network behaviour analytics.

According to Fortinet's Khuffash, there are several skills required to operate a successful MSSP practice, however, it depends on the services being offered.

Khuffash said most importantly, having knowledge of a security operations centre (SOC) is critical as it is one of the main components of a MSSP practice. "Knowledge of different firewall vendors and how to apply the necessary rules and policies on them for maximum security posture is key in delivering such services," he said. "It is crucial that channel partners invest in training and certifying their staff continuously to ensure they are successful in delivering the services their customers expect from them."

eHosting DataFort's Zeineldin noted that managed services are in general built around service level agreements (SLAs) and it is important that deputed IT personnel are aware of these terms. "This calls for an effective balance between getting the job done and remaining within the billable hours to guarantee ROI," he said.

He explained that cyber security is now, to an extent, being governed by regulations and this calls for several compliance issues which need to be tackled to maintain industry standards. "Achieving compliance certifications is a long drawn process but nevertheless a necessity," he said. "MSSPs must be consistent in their efforts in working towards these certifications. They must have the necessary procedures and people in place to ensure that they are up to date with these requirements.

> *Being a partner of expertise and not a 'me too solution provider' will differentiate your offerings in the market. Sometimes you have to let go when a customer is not willing to budget for IT security for whatever reasons, but expects protection against the most sophisticated cyber threats.*
>
> **DIPAK VAGADIYA, SECURITY LEAD, EMITAC ENTERPRISE SOLUTIONS**

Harish Chib, vice president, Middle East and Africa (MEA), Sophos, said the transition to next-gen IT security MSPs, often called managed security service providers has been a challenge for channel partners to operate successfully in this new and far more complex environment. Chib said clients are no longer tied to one machine, one server, one location and the corresponding IT security needs of those clients have increased accordingly.

"Channel partners must find a better way to manage licenses by using a billing and licensing option, where you can distribute licenses across multiple customers in a more flexible manner—like an aggregate monthly billing option—will speed up the services that are being offered and will be ready to evolve and meet the needs of the customers if those needs grow (or shrink) unexpectedly," he said.

Given that security is a highly sensitive area of business, to build a good MSS practice, solution providers primarily must strengthen trust within existing and potential customers. This is especially important, as the customer is placing their critical data with the security provider.

Khuffash noted that in order to meet the demands of new networking models being adopted by customers, many providers need to evolve their managed service offerings to align with the elastic and agile infrastructure and application delivery models, such as public clouds and SaaS, IaaS that many organisations are implementing.

He said the maturity of the MSSP market will be based on the portfolio of services providers in this sector offer along with the proper pricing model being offered to their customers. "Most MSSPs are offering the service as a monthly subscription bundled with connectivity if the MSSP is from an ISP background. Other MSSPs offer customer premises equipment (CPE) at the customer site where it is remotely managed through a lease to own package with a management fee," Khuffash said. "I have seen other MSSPs that are now offering packages on their cloud-based on newly introduced models such as consumption base, customer pays on traffic that is inspected only."

Emitac's Vagadiya said every organisation needs help with managing its security operations. He added that whether companies build their own security operations and run those internally or out source, it is critical that they work with an

expert in security services.

However, Vagadiya said most solution providers lack detail of covering the customer from threats and that's one of the issues that solution providers should consider when building a managed security practice. "As threats are dynamic, serving few quality customers than trying to protect the whole globe with services is the best way solution providers should go about building their managed security practices," he said.

Chib pointed out that technological advancements, in terms of hardware, software, and user needs, have altered the workflow and landscape from the previous generation of MSPs. Security has become all the more complex, and the knowledge-base MSPs must have at their disposal has become accordingly more complicated, as businesses turn to the cloud and web-based resources to manage their products. "Clients are no longer tied to one machine, one server, one location, and the corresponding IT security needs of those clients have increased accordingly," he noted. Business owners and their employees, have increased their security needs exponentially by not only decoupling from the physical office and taking their work home and on the road, but by also spreading it across multiple devices."

He said MSSPs must now have the capability to protect not just desktop computers, but laptops moving from location to location, easily portable tablets and smartphones capable of handling the workload once limited to a desktop machine.

Vagadiya agreed with Chib on MSSPs having the right capability to provider security services and observed that anyone who has not spent years in information security operations, cannot get the managed security services business model right. "The only people who got this right are the ones with hands on experience in the security segment," he said.

He explained that solution providers should focus on building teams of experts and need to stay with few customers to start with for a couple of years before they go all out announcing their expertise in this sphere. "Having experience in the domain is most important because this business cannot be built over night," he said.

Vagadiya explained that channel partners should validate and help customers understand the value of the quality. "Here 'cheapest is best', and may sell but never bring a repeat client," he advised.

Vagadiya said knowing what you are reselling like not suggesting buggy software to your customers or sell cheap security services is one sure way of maintaining your reputation and providing quality offering to customers. "Being a partner of expertise and not a 'me too solution provider' will differentiate your offerings in the market," he said. "Setting customers' experiences and making sure to right size the coverage is crucial for success. Sometimes you have to let go when a customer is not willing to budget for IT security for whatever reasons, but expects protection against the most sophisticated cyber threats."

Zeineldin said the main issue today is to utilise the existing investments made by the customer rather than replacing it and add additional security solutions which may be offered as multi-tenant shared services, which would otherwise add to the cost for the customer.

He said while some companies may opt to be niche players in the managed security market, others choose to add the practice to an already existing managed services business model. "For example, eHosting DataFort has been in the cloud hosting and managed infrastructure market for a long time and we have seen a huge demand for managed security services over the last few years," Zeineldin said. "In our case it was a natural progression towards building a MSS practice to offer our current customers and to tap into the growing potential customer base."

However, Zeineldin emphasised that it must be understood that, unlike a sales-oriented model, the approach to interacting with customers must shift towards being more service-oriented, where customer expectations are very different.

Eldeeb said since the responsibility to install, configure and manage security products that organisations need is on the solution providers, they need to understand the relevant regulations and apply best practices and reporting.

Eldeeb added that solution providers must provide the reliable guidance, active monitoring, and rapid responses to mitigate security incidents and compliance for these organisations.

"For partners trying to differentiate themselves at a high level, the greatest challenge will be recruiting staff with the appropriate data analytics skills," he said. "Organisations are aware of their limited capacities to protect their IT infrastructure from increasingly sophisticated cyberattacks and want to spend their valuable time focussing on tasks that drive real business value."

Aside from that, Eldeeb explained that solution providers need to be both flexible and savvy. "For example, an organisation may need to add a firewall or a management system to its portfolio," he said. "A provider can use these opportunities to generate additional revenue through equipment sales or leasing."

Zeineldin pointed out that because managing security requires a serious amount of time and dedication for the business to be profitable, a significant amount of automation which can ease the day-to-day navigation processes is vital. "With IT skills becoming more crucial and quite often limited in numbers as well as quality, MSSPs must be able to utilise such processes more efficiently," he said. "Diverse technology footprint across different customers becomes essential as a service provider to have expertise across these technologies."

Zeineldin added that: "Typically, when we onboard a customer, coping with the noise in terms of alarms becomes an issue. However, it eventually helps streamline the use cases to be more relevant to the customer environment and provide a better context so that any alarms triggered can be better addressed by our cyber defence centre (CDC) analysts." ■

MSSP BUSINESS MODEL

Getting the business model right around managed security services is still a challenge for some channel partners mainly because managed security is not a single product. Here are some tips from industry experts on how to go about

Be a virtual CIO: Clients are entrusting the security of their greatest assets—their data—to the MSP. A successful MSP will be able to provide both the high-level and user-level guidance the client needs, acting as a resource for the answers, software, hardware, and more

Be a service differentiator: Meet the modern client's needs by being constantly available, wherever they are—and wherever you are—through a SaaS-based management console. The right tools will give you the flexibility to match your clients' mobility.

Next-gen MSPs must align their security strategy with vendors. Vendors, meanwhile, need to become more integrated into the MSP vendor ecosystem, developing and providing tools MSPs use to run their business (PSA) and remotely monitor and manage (RMM) for their customers.

Be a proven security differentiator: Ensure your tools provide top of the line security and protection. Your customers are able to offer secure, uninterrupted service for their users because you've got them covered against outside threats. By finding and working with the right vendors—and by providing them with the education they need to make best use of the tools you provide them—an MSP can be the first and last line of defence against cyber threats.