A SAFE BET

IS MANAGED SECURITY SERVICES RIGHT FOR YOU?

With increased protection against an ever-changing threat landscape becoming a must-have, many enterprises in the Middle East are turning to managed security services for help. For CISOs who are struggling with a bewildering array of in-house point security solutions and skills shortage, managed security service providers (MSSP) offer a compelling value proposition.

According to IDC, global spending on managed security services is expected to reach $21 billion this year, as more and more organisations turn to MSSPs for security capabilities and consulting services.

"Managed Security Service Providers (MSSPs) are becoming increasingly popular with each passing day. Organisations of varying sizes are relying on MSSPs to prevent potentially devastating cyber-attacks. Furthermore, leaning on the digital security professionals for assistance reduces the workload burden on in-house IT personnel and help with cyber-security challenges," Yasser Zeineldin, CEO of eHosting DataFort.

Yasser Zeineldin

Simon Willgoss

He says organisations opt to work with MSSPs for several reasons. Some are concerned that their in-house tech team resources are insufficient. Others lack the relevant expertise provided by the security professionals at MSSPs. In some instances, companies hire MSSPs to perform comprehensive security audits or respond to particularly challenging incidents.

In agreement, Simon Willgoss, Head of MSS, Help AG, says the two main factors driving managed security services adoption are access to expertise and cost-efficiency. Managed Security Services help move IT budgets from intimidating CapEx to more manageable OpEx while at the same time transferring specialised security activities to a team of qualified security experts. This is especially helpful in the Middle East, wherein the lack of skilled cybersecurity professional is a pressing concern.

"The pay-as-you-go model lends itself to both upward or even downward scalability. Finally, availability is also a factor as with an MSSP; the customers get 24x7 support with assured 99%+ availability which ensures that business is always on," he says.

In mature markets, for small and medium-sized enterprises that can't afford a full-time CISO, some of the MSSPs have also started offering CISO-as-a-service as a cost-effective alternative. This trend is slowing catching up in the Middle East as well.

Harish Chib

"We see the role of a virtual CISO to be played by MSSP. Clients are entrusting the security of their greatest assets—their data—to the MSSP. A successful MSSP 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 and act as a virtual CISO for organizations," says Harish Chib, VP-Middle East & Africa, Sophos.

"FINDING AN EXPERIENCED CISO THAT UNDERSTANDS THE ENVIRONMENT AND HAS THE ABILITY TO GET CHANGE IMPLEMENTED ACROSS AN ORGANISATION IS EXTREMELY HARD. A CISO (AS-A-SERVICE), CAN WORK WITH A CIO TO ENSURE THEY HAVE AN UNDERSTANDING OF THE THREATS THAT ARE FACING THE ORGANISATION AND HOW TO PROTECT AGAINST THEM. THE CIO WOULD HAVE TO FULLY SUPPORT THIS MODEL, AS THEIR BUY-IN IS ESSENTIAL FOR SUCCESS."

Matt McCormick, SVP Business and Corporate Development, ThreatQuotient, echoes a similar opinion: "Finding an experienced CISO that understands the environment and has the ability to get change implemented across an organization is extremely hard. A CISO (as-a-service), can work with a CIO to ensure they have an understanding of the threats that are facing the organisation and how to protect against them. The CIO would have to fully support this model, as their buy-in is essential for success."

The increased demand for managed security services has resulted in many VARs and SIs adding security as a service to their portfolio. With many choices available before them, there are some key criteria for users while evaluating an MSSP.

"Technological advancements, in terms of hardware, software, and user needs, have altered the workflow and landscape for MSSPs. Security has become all the more complex, and customers should look for MSSPs with huge security knowledge-base. The knowledge-base MSSPs 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," says Chib from Sophos.

Willgoss from Help AG adds the unfortunate reality of cybersecurity today is that no system can be 100% secure and security breaches are inevitable. Hence , Incident Response with a mix of onsite ("boots on the ground") and offsite experts is a must. "CISOs must consider the MSSP's incident response SLAs to understand how soon (hours/days) they can assign resources and ensure availability of experts.

"To successfully deliver security services, MSSPs will also almost definitely need to login to the client's environment remotely. CISOs must, therefore, consider what kind of

visibility and access they can expect their MSSP to require and whether they can provide records of their access. Also, CISOs must have a clear picture of what their MSSPs' resources are doing and when," he adds.

Ronen Shpirer

According to Zeineldin from eHDF, to ensure that there is a clear demarcation of expectations and deliverables, companies must look for well-rounded service-level-agreements which highlights the services and implementations. It will also need to include the processes and systems that will be put into place for daily work requirements. Given budgets allocations, organisations must be able to understand the flexibility provided by the MSSPs depending on usage patterns as well as the provision of 24x7 security monitoring and management.

Ronen Shpirer, Senior Solution Marketing Manager, EMEA at Fortinet, says it is also important for MSSPs to examine the enterprise technology stack – both on prem and cloud – of customers to identify vulnerabilities. "Providing silo solutions, or security services based on silo solutions (as is still done today for some MSSPs), s very complex and costly to deploy and manage. It introduces possible security gaps and limits the ability of automation and agility. MSSPs should evolve their service delivery infrastructure so that security visibility and services are delivered end-to-end with a maximum of integration, automation, and openness via open APIs. "

With managed security services gaining steam in the Middle East, an important question for everyone in the industry is whether your MSSP is liable for damage if an incident occurs. In developed markets, the liability of exposure can run into multi-million dollars. However, it remains a grey area in the region.

"The liability of an MSSP is always capped, as, unfortunately, there is no way to 100% protect customers from cyberattacks. Many times, customers further protect themselves by having Service Level Agreements (SLA's) with their service providers to ensure proper response times, etc.," says McCormick from ThreatQuotient.