Magazine Article | October 2, 2017

The MSSP (R)Evolution

Source: Channel Executive Magazine

By Lynn Souza, owner, CEO, and president, Connect Computer

These days, every third email I receive is about the MSSP space, and every other article I read is about cybersecurity. So why have seemingly so few companies made the transition from MSP to MSSP?

The statistics on cybersecurity and cyberattacks are overwhelming:

- According to the FBI, cybercriminals are expected to collect over $1 billion in ransoms this year.
- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016.
- The average cost of a security breach is $4 million, and that is expected to exceed $150 million by 2020.
- 44 percent of businesses estimate they could lose $10,000 or more during just one hour of downtime.
- Cybercrime will cost businesses over $6 trillion by 2021.
- Global cybersecurity spending was just $3.5 billion in 2004. This year it is expected to be $120 billion, and by 2021, spending on cybersecurity is expected to reach $1 trillion.

Over the last few years, enterprise corporations have been adding cybersecurity professionals to their payroll, and in 2016, the CISO (chief information security officer) role became the hot new executive position. In fact, in September of last year, the White House even jumped on the CISO bandwagon and announced that Brigadier General (retired) Gregory J. Touhill would become our nation's first federal chief information security officer.

Considering the already immense shortage of qualified cybersecurity experts (a recently published article by Forbes, ISACA, a nonprofit information security advocacy group, predicts there will be a global shortage of 2 million cybersecurity professionals by 2019), enterprise corporations have been recruiting some of these experts away from smaller companies, leaving a massive shortage of talent in the SMB (small to midsize business) market. Even if an SMB is lucky enough to find a qualified cybersecurity professional, affording to pay that individual would prove very difficult.

Much more than enterprise companies, money is a huge factor in SMBs' inability to hire and/or retain cybersecurity professionals. An average cybersecurity professional garners a $90,000 salary, while the average salary for a CISO averages $204,000.

"The SMB market is not only wide open for MSSPs, they are also the most in need of security services."

Taking into consideration both of these factors, the SMB market is not only wide open for MSSPs, they are also the most in need of security services. A recent analysis showed that small and midsize businesses of up to 1,000 employees have a 63 percent higher risk of a data breach than larger organizations. Couple that with the fact that 60 percent of small businesses close after a breach, and the undeniable conclusion is that implementing cybersecurity policies and technology is truly a life or death situation for small and midsize businesses.

NEW SECURITY SKILLSETS REQUIRED

While the transition over the last 10 years from VAR to MSP was not necessarily an easy one, the IT skills required for both were relatively the same. To be a VAR or an MSP required top-notch IT professionals that could scope, install, configure, and support corporate infrastructures and WANs. Of course, learning a new set of tools to deliver managed services was a hurdle to overcome, but again, there wasn't a huge learning curve required by the existing group of IT professionals. That has all changed with the evolution of the MSSP. Most IT professionals understand the concept of security and can deliver some cybersecurity services, such as configuring a firewall for geo-IP filtering, monitoring

"Making the jump from VAR to MSP was evolutionary, but the next jump from MSP to MSSP is truly revolutionary."

and auditing; antivirus/antispam; and security patching, but those same professionals do not have the skillset required to conduct and assess vulnerability scans, penetration tests, or perform forensic investigations, just some of the services that are a requirement if you want to truly compete in the world of MSSPs.

The vCIO role is one highly touted by top MSPs; however, transitioning to an MSSP will require having the virtual role of vCISO to offer to clients. vCISOs will be responsible for creating security policies, controls, and cyber incident response planning; ensuring compliance with the changing laws and applicable regulations; and maintaining a current understanding of the IT threat landscape, among other responsibilities related to the security posture of their clients.

COMPLIANCE REQUIREMENTS CREATE OPPORTUNITY

Compliance is another huge growth area for MSPs transitioning to MSSPs, and it will only continue to grow as the inevitability of more regulations comes to fruition. At the end of 2016, New York became the first state in the nation to create a cybersecurity regulation. 23 NYCRR 500, as it is known, was created to ensure that financial services entities do their due diligence in protecting their customers and information systems against cyberattacks. Rest assured, more states will follow suit, creating more need for MSSPs to know and handle compliance and provide cybersecurity services. Perhaps the most sweeping global cybersecurity legislation to date was passed by the European Union last year and goes into effect in May 2018. The GDPR (General Data Protection Regulation) applies to any company that does business with EU residents, regardless of where the company resides. Even if the company is offering a free service, such as a website that people in the EU access, a company may be subject to GDPR if it collects IP addresses or tracks cookies. A survey done by Pricewaterhouse Coopers showed that more than three out of four (77 percent) U.S. companies plan to allocate $1 million or more on GDPR readiness and compliance efforts, with 68 percent saying they will invest between $1 million and $10 million and 9 percent expecting to spend over $10 million to address GDPR obligations. Combine these new compliance regulations with those already in existence like HIPAA, PCI, and FFIEC, and there are millions, if not billions, of dollars to be spent (and made) on cybersecurity services.

As successful MSPs have gotten great traction in the SMB market, and they are adding MRR (monthly recurring revenue) consistently, there is a huge mountain to climb (and admittedly a little bit of fear) to enter the MSSP space. The talents required and tools needed to be able to effectively deliver a full suite of security services involve a significant investment of time and money. Decisions need to be made: Do you recruit and hire a cybersecurity professional or do you take the longer road of sending current staff out for training, thus delaying your ability to deliver security services for at least another 12 to 18

months? What software do you choose, as every day there are more and more vendors entering the cybersecurity space? Eight cybersecurity companies made the Inc. 5000 list this year, and the old stalwarts of antivirus, like McAfee and Symantec, are now trying to keep up with companies like Carbon Black and Cylance that go beyond traditional antivirus and use artificial intelligence and machine learning to identify malware before it can execute.

Making the jump from VAR to MSP was evolutionary, but the next jump from MSP to MSSP is truly revolutionary. If you are not already in the process of transitioning your company to deliver managed security services, then either start investing immediately or go out and partner up with another company or vendor that can help you provide those services before your clients start getting lured away by your competitors that have made the conversion to MSSP. In the not-so-distant future there will no longer be MSPs and MSSPs; there will be providers that offer end-to-end security and compliance solutions and providers that no longer exist.