MID-SIZED COMPANIES & THE MSSP PROBLEM

RON BURLEY
Security Engineering Director, Netelligent
Security ….

Throughout a business' life, there are a few stages that can signal prosperity: The first dollar made in a small business, hitting the first 100 employees for a slightly larger business, and the first cybersecurity breach for any size company. The thing with these milestones is that they are inevitable as the company grows. You WILL make that first dollar, you will (hopefully) hit that 100th employee, and you most assuredly will have a breach of some sort.

The problem, of course, is the focus of a company as they continue their growth. Money is, and should, be spent on activities that will help the company grow. Rarely does cybersecurity become a talking point before the IT department is solidified to support critical systems. And never does cybersecurity become a talking point before the company is in the black.

Companies focus on growth and yet attackers rarely care about the success of a company.

Therein lies the problem: while the focus of the company is on growth and the activities that directly affect that, attackers rarely care how far the company has come. In actuality, they may even focus on the fact that a company has decent growth and see them as a softer target.

So what does a company to do? Spend a premium on a security specialist (and yes, we do come at a premium)? Try to encourage an IT staffer to start focusing on security? Farm out the detection and response process to a 3rd party? Or maybe push any of those costs off for another month, just to make sure the numbers are a little better?

Alarmists will tell you that security spend is devastatingly low for ALL sizes of business and it must be increased immediately! Others will tell you that 75% of all spear-phishing attacks targeted SMBs[i]! Others will even tell you that the end of the world is nigh and security breaches are the death knell of the world (ok, those people might be a little more than

alarmist…). The point is, a significant amount of people are attempting to scare mid-sized business into spending budget they probably don't have and which may even risk the ability to continue to grow.

When it comes to security professionals, this is where we tend to split. Many believe that security spend should be your #1 priority and never be outshined by anything else[ii]. While many don't refute that security spend is important, I don't believe that it should be weighted more than critical business needs or growth opportunities.

Even with a limited budget, invest and increase the security education level within your organization. Don't skimp.

It's not necessarily the spend that should be increased, it's the education level. I've worked for a lot of organizations that sell security services, and the one thing that concerns me about midsized companies is their apathy toward learning why security is important. I'm not asking anyone to become a white/grey/blackhat hacker, I'm simply asking them to understand what it means when malware infects a device, how it might try to move laterally, what activities it takes in the process of covering its tracks, and what the REAL effect on the computer/user/company will be.

I don't necessarily agree with midsized business attempting to grow their own cybersecurity group internally at the cost of other business needs. Educating yourself is one thing, but hiring a whole team is quite another. Even the hiring process is risky for midsized companies if they want to try to start a security group. If you don't understand the basics of breach anatomy, or even the products that are meant to detect them, how can you validate the applicant knows either? The glut of security opportunities has polarized the security talent pools in this country: there is NO unemployment for cybersecurity professionals that have the skills necessary to do the job.[iii]

Unfortunately, that means as the experienced professionals are hired, a glut of inexperienced resources are flooding the market[iv]. This makes things even harder for midsized business to hire. So, what's to be done about the gap? MSSPs. Managed Security Solution Providers have been around for as long as there have been security breaches. Nature abhors a vacuum, and we definitely filled a necessary gap. Unfortunately, as with everything, the solution itself introduces a significant amount of problems.

Notably, most MSSPs are not the same. When you start looking at providers in Gartner's "Magic Quadrant" reports, you see huge organizations like NTT Security, Verizon Business, and Dell Secureworks. While these are very reputable companies, their sights are fixed solely

on Fortune XXX companies. Granted, some of them have smaller offerings, but there is a high probability their focus will reside with the larger organizations.

So, this leads us to the MSSPs on the lower end of the size spectrum, and boy are there a lot of them! Each of them are trying to eek a little business out of a growing market, reflecting on their own offerings and trying to differ from each other in even the slightest way possible. Throwing terms out there like "advanced security data analytics" and "senior cybersecurity resources" that will peer into the very soul of your company's network looking for malicious intent. All marketing fluff, tried and true. So, what ARE you supposed to look for and what questions should you ask when selecting a midsized MSSP?

Here are a few questions and the answers you should be getting from them. Bear in mind, some smaller MSSPs won't be able to answer these questions because they don't have the ability to execute, but look for plans in their answers if they don't have what you are asking for right now.

Question 1: What type of threat intelligence do you ingest, create, and/or share?

Look for them to talk about their own methodology in understanding what threat intelligence even is. A good reference for you to read before you ask the question is here: https://thehackernews.com/2015/11/what-is-cyber-threat-intelligence.html. Look for them to also talk about using indicators of threat (IoT) that they themselves collect based on what they are seeing in the customers they monitor, and how they report this back to you. Is it a monthly report? Ad hoc alerts when they see issues? Part of a QBR with you to talk about your own threat posture? Essentially this: they should understand threat intelligence, know that it helps with detection, know where they are getting theirs, and have a plan on how to share this information with you on a regular basis.

Question 2: What type of SIEM and other products are they using for detection and alerting, and what is their methodology for detection and alerting?

The one thing you're not looking for here is "best of breed" products. What you are looking for is the fact that the MSSP has a method to their detection madness, and know what to do when they see an alert.

A Security Information and Event Monitor (SIEM) is absolutely necessary and should be a

backbone of the MSSP, but they should not be 100% reliant on it. They should have other processes around how detection is done, how they correlate and validate alerts (i.e. with the aforementioned Threat Intelligence), and a validation process to make sure that the alert is not a false-positive. For more advanced MSSPs, they should also have a response "run book" or, at the very least, an avenue to be able to provide you with remediation around that alert.

Question 3: What is the experience of the analysts, investigators, security specialists?

Depending on the MSSP, they may have a decent hierarchy (starting at level 1 analyst and possibly going all the way up to an investigator or researcher), or they may have a very flat organization in which a handful of people do pretty much everything. Neither is inherently good or bad, but it will show you what you can expect from them in the realm of information and action.

A hierarchized organization will be more specialized and assumed experienced, but there will be additional processes as an issue is escalated through the organization. A flatter organization will have, on average, more personalized services but may lack in knowledge depth. This is especially evident when a flat organization has one expert (or "rockstar") on staff and they are constantly being escalated to. If there is one specific thing to look for it would be the amount of experience for each level. While a Masters of Cybersecurity is an impressive sounding degree, it is only a foundation. Security is learned in the trenches and being able to stomach multiple failures before you get the thick skin necessary to keep cool during a breach. As much as they try to simulate that in school, there is no comparison. Actual security experience in the field is what is important.

Question 4: What communication and reporting will I receive as part of this service?

This is one of the most important questions you can ask. Everything that an MSSP does (detection, hiring, experience) culminates in what they communicate back to you! You're looking for sample reports and notifications that can give you an idea of what you'll be getting. If they are unable to provide you with one, or say that they are "designed on a per-customer basis" then you should run immediately. Additionally, look for them to talk about how they notify you of an alert, whether the communication changes based on severity of the alert, and the quality of detail that is provided. You should also be looking for value-adds like quarterly

business reviews (QBRs), regular cadence on trends they are seeing in your alerting, and general discussion around security trends as a whole.

---

[i] The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

[ii] Observation based purely on conjecture and discussions I've had with many security professionals

[iii] Cybersecurity Unemployment Rate Drops to Zero Percent http://cybersecurityventures.com/career-news/

[iv] Fewer Than One-Fourth of Cybersecurity Job Candidates Are Qualified http://www.darkreading.com/vulnerabilities---threats/fewer-than-one-fourth-of-cybersecurity-job-candidates-are-qualified/d/d-id/1328244