

Quantizing Managed Services – What are we “Missing” by NOT Having It?

When asked recently by a customer why Managed Services was so important, and what they would be missing without it, much to their surprise, my answer was “EVERYTHING!!!”

Could you be more specific, they asked, as so I was. Below is just one small collection of items that make Managed Services “worth its weight in gold”.

1. **SPAM Attacks with “INTENT”** – while the majority of the SPAM that gets delivered on a regular basis to end user mailboxes worldwide, is nothing more than junk mail, there are those occasional emails carrying viruses or malware, with the “INTENT” of infecting an end user’s system, behind the company firewall. With this infection, a hacker can very quickly (1) escalate his/her privileges locally or domain-wide on the company’s network, (2) install key-loggers to steal passwords from systems or attempt hacking the local SAM within Windows on each system to steal passwords (which passwords may also then be used elsewhere, for those users that keep a single password for multiple systems or programs), (3) install software or code (like a BOT or Backdoor for example) that will allow future remote control of the system with very little effort, (4) steal product keys, (5) launch attacks (like a Denial of Service attack, for example) against local systems or even other company’s assets, (6) steal data, (7) corrupt data, (8) modify the operating system in such a way that makes it unstable or liable to crash, (9) steal personal information (like social security numbers, names and addresses, or patient information, in HIPAA environments), (10) steal customer lists (i.e.; the names of customers, addresses, primary contacts, methods of contacts, annual sales, etc...), (11) steal proprietary company data (in the case of corporate espionage), (12) steal money, or bank account information used to that end, and the list goes on.

Now let’s assume you’ve been targeted by a hacker, how would you know? The answer is if you’ve received a virus (or at least an attempt to plant a virus). So how would you know? Well one way, would be to check SPAM firewall software or appliance logs, if you have such a thing protecting your network. A second way would be to check firewall logs, if your firewall has IDS (Intrusion Detection System) functionality. But even with both IDS in a customer’s firewall, and a high-end SPAM firewall, the pure fact of the matter, is that IT people (staff) very seldom do anything more than glance at a web-based report from their SPAM firewalls, or review firewall logs whenever they access a firewall and aren’t in a hurry to do something else (perhaps once every 3 months, if that). What’s the problem with this approach, if the SPAM firewall blocks the virus in an email in the first place, right? Wrong!!! Hacking often involves repetitive attempts to gain access to a company’s network, until the hacker’s goal is ultimately reached. For example, a hacker doesn’t try entering a password thru an RDP (Remote Desktop Protocol – Used for legitimate remote access to the Windows Operating System by technical staff or end users, for those unfamiliar with this acronym) session once, twice, three times, and then gives up. Rather, they run a brute force attack, where they’ve

automated continual attempts using specialized hacking software. Very often, a hacker might setup a program to run, and come back weeks later, when it's had a chance to do its job. Hence, one could very astutely conclude that it's important to catch hacking attempts early, so as to stop all attempts, before they can be successful. So back to our theme "Managed Services – What are we missing without it". One answer is the ability to be notified of hacking attempts, so that you can take action against them as soon as physically possible.

For example, our business has a Fortinet firewall in place, protecting the perimeter of our infrastructure, within a secure data center. As part of a software bundle included with the unit, is antivirus software, which provides an additional layer of antivirus protection, at the gateway to our network. When encountered, a virus will be cleaned, and then the details of said virus, will be recorded to a log within the firewall. As soon as those details hit that log, a second log entry is recorded in our managed services database, followed by the sending of an email alert to our service department. From there, a technician can record (and look up) the source IP addresses from whence the virus came, and create a new policy on our firewall to block future traffic from said IP address. So to further elaborate, in a recent attempt, we found a hacker that sent a virus to us from somewhere in Amsterdam. When we compared alerts from our SPAM Firewall software, for viruses originating from SPAM emails, we quickly determined that this was this individual's 4th attempt at infecting internal users on our network. Each time, they modified their approach slightly, via some other form of advertisement displayed within the body of the email message, varying their message's subject line, etc... In response, we created a new policy to block all future access from the IP address specified, which at the same time stopped a significant amount of SPAM that we were getting, as this individual apparently infected someone else's network, and was doing SMTP relays from their mail server. As a result of our inquiry, this company was also able to realize the infection that existed on their own network, was able to clean it, and was able to resolve email issues they themselves were having (due to being put on various blacklists, because of the hacker that was spamming from their carrier-allocated external IP address).

- 2. Hacking Attempts at Points of Remote Access** – Almost every IT guy at some point realizes the benefit of remote access, and in response implements RDP access on servers or workstations that they themselves are responsible for maintaining. But what about when a hacker stumbles across this configuration and starts trying to hack their way into that RDP access? If the IT guy doesn't have security auditing configured, to record these hacking attempts in the Windows Security Logs, the company will never even know these hacking attempts are happening. As a result, the hacker has as much time as he/she could desire, to brute force their way into the company's network. Furthermore, if group policy doesn't exist in the form of account lockout policies, then the hacker can try as many passwords as they like, without anything to hinder their attempts (like the accounts they're attempting to use being locked out, for example). Let's assume, however, that your company has both auditing and group policy

configured, to lock accounts and record failed login attempts. How's the IT guy going to know that a failed login attempt occurred, or when someone's successfully hacked their way in, escalated their privileges, created or deleted accounts, and so on? The answer is whenever they get around to actually checking the Security logs. Even if the company has an IT provider that comes out once a month to check their systems, that's way too late to (i.e.; once a month) be responding to such a threat. That said, without Managed Services, you "Miss" the ability to know: (1) when failed login attempts occur as they happen, (2) when account privileges are escalated for an account, (3) when someone attempts to reset a password, (4) when a new account is created, or when an account has been deleted, and (5) when accounts have been locked out due to too many consecutively entered, incorrect username and password combinations. Armed with this knowledge, and as with the SPAM example above, an IT guy can block future hacking attempts, by creating a policy on the company firewall to block all traffic from a given IP address. They can also determine when new accounts have been created, and delete or disable said accounts, to remediate unauthorized access that may have successfully been achieved by a hacker.

- 3. Carrier Services Deficiencies** – If your Internet service provider experiences regular packet loss or latency, how do you know about it? Furthermore, once you find out about it, how do you record statistical information about what's transpiring with regard to your connection, so that you have ammunition to do something about it (For example, so you can break a lengthy contract with an IS, without being stuck with an ISP, or without being fined, or without having to pay for two carriers if you can't manage to get out of your contract)? Without managed services, you are "Missing" the ability to do any of these things, and in essence, are unable to get accountability from your ISP. Something else you're missing, however, is free diagnostics for those connections your company has from varying ISP carriers. So to conclude, and in comparison, if you have just 2.4 outages per year from your ISP carrier (without including other important information collected about the connection, like latency and packet loss, which could help diagnose other performance-related issues, such as slow Citrix sessions), managed services has paid for itself.

Ex. 2.4 Outages multiplied by 2.4 service calls with 1 hour minimums, at a rate of \$85/hr = \$204/year

And

\$34/mo x 12 months = \$408/year for managed services coverage of your Internet connection.

If you conducted a survey, you'd more than likely have a very high percentage of companies tell you that they've had at least 2 outages (if not more) each year. But then let's also consider how long it normally takes to determine whether you're having an outage. Multiply that time, by the total number of users you have, and the hourly rate

you pay them (or are now paying them to sit around, perhaps unable to be productive), and you'll very quickly see that one single outage could result in a greater cost (due to hindered or halted productivity) than the entire annual cost of managed services for your Internet connection. So in essence, being able to determine and report to an ISP Provider that you're having an Internet outage within say 5 minutes, versus an hour, and not having to pay for the diagnostics associated with making that determination (as 15 minutes worth of free diagnostics time is allocated to every alert reported for every managed services customer), means that managed services very easily pays for itself, and then some (at least for your Internet connection, as you can see here). So I guess in conclusion, we could also make the case that without managed services, you're missing (1) a significant cost savings, from an IT diagnostics perspective, (2) hindered or halted productivity, resulting in hundreds or thousands of dollars lost each hour, (3) accountability from your ISP Provider, and (4) the ability to have evidence that your ISP Carrier is not living up to their SLA, thereby giving you ammunition to use towards breaking your contract with them (should the need arise).

- 4. A Reduction in Preventative Maintenance Costs** – The average IT Provider charges \$85/hr for Field Service Engineer-level support (some IT providers charge as much as \$140/hr), within which the realm of performing Preventative Maintenance would fall. And, the average time spent each month performing preventative maintenance tasks (i.e.; running disk defrags, disk cleanups, removing cookies, removing temp files, checking antivirus logs, checking backup logs, removing temporary Internet files, checking System Event Logs, doing performance analysis via tools like Perfmon, etc...), is 30 minutes to an hour or slightly over, per system, per month. This time varies, however, depending on: (1) whether the system is a workstation or server, (2) how many resources are available on the system for performing preventative maintenance, with regard to CPU and Memory, (3) how fast the company's Internet connection is, (4) how many updates are needed on each system, (5) the size of the individual updates to be downloaded and installed, and so on.

So if we do some basic math, we very quickly see that utilizing Managed Services in place of manual preventative maintenance is more cost effective (not even taking into consideration that fact that manual preventative maintenance is a "Reactive Approach", and not a "Proactive Approach", and as such results in more downtime for customers, due to its lack of 24x7x365 monitoring). For example, let's say it only takes 1hr per system, per month, to ensure proper "Manual" preventative maintenance is performed (at least once a month that is), and your rate for that support is \$85/hr. A company with 30 devices would then pay \$2,550/mo for "Manual" preventative maintenance on 30 systems.

Ex. That's \$85/hr x 30 hours of billable labor = \$2,550

The same cost for preventative maintenance under our Managed Services offering (which is by itself just one of the benefits of our Managed Services offering, in addition

to 24x7x365 monitoring, alerting, reporting, trend forecasting, remote access, etc...), for 30 devices, is \$1,190.

Ex. That's \$34/mo x 30 devices, plus 2 hours of Monthly Management Time at \$85/hr = \$1,190, or **a savings of \$1,360/mo**, minimum, without including the 15 minutes of free response time per incident, provided with our managed services offering.

So as you can see, without Managed Services, you're "Missing" the ability to save nearly 50% each month, in preventative maintenance costs alone.

5. **A Reduction in IT Support Costs** – The average customer without a Preventative Maintenance contract or Managed Services contract is subject to a 1 hour remote access, or 2 hour on-site minimum charge, for all IT support. However, under our Managed Services plan, customers are billable in 15-minute increments, and no minimums apply, with the exception of on-site support, for which we require minimums to cover our technician's travel time, and mileage reimbursement. Hence, for those issues which can be resolved within 15 minutes (of which many issues fall into this category), and which were identified within our managed services platform, a company saves:

- A. A minimum of \$85 per incident in remote support costs, or
- B. \$170 per incident in on-site support costs.

Furthermore, for those issues alerted on in Managed Services, requiring 30 minutes of support (for which the first 15 minutes of support are still covered free of charge), a company saves:

- A. A minimum of \$63.75 per incident in remote support costs, or
- B. \$148.75 per incident in on-site support costs.

So to sum up, without Managed Services, a company also "Misses" hundreds or thousands of dollars worth of savings, annually, in general IT Support costs. After all, if a company has 60 issues in a year's time (not unreasonable), and even if only half of those issues are diagnosed thru managed services, then that company is saving \$1,912-\$5,100/year in IT Support costs, on the low end.

Important: This statement is very accurate, especially considering the fact that over 90% of all issues can be diagnosed in part or in their entirety, from the information collected by our Managed Services offering (whether they are security-related, application-related, operating system-specific, performance-related, and/or hardware-related).

6. **A Reduction in Lost Productivity** - At some point on every system running on a company network, resources will have to be added, to accommodate additional load being placed on a given system, due to the addition of applications, and/or connections from local or

external end users (i.e.; in the form of remote access connections, end user's opening files within a shared directory, Citrix or Terminal Server sessions, etc...). While this is common sense, what most people don't know, is how long end users put up with poor system performance before finally complaining about it (which while left unchecked, is hindering their productivity, and thereby costing a company additional monies, where no additional work has been performed). Hence, as you can see, without Managed Services, a company "Misses" the ability to see exactly when there is a resource shortage on a desktop, laptop, workstation, server, firewall, router, you name it, so that resource shortages can be remediated, thereby restoring proper productivity levels for employees, and reducing costs. For example, if the average end user spends an extra 10 minutes each day (which is not by any means un-reasonable) waiting for their computer to boot up, or waiting for programs and the operating system to respond, due to Memory or CPU shortages, those shortages (assuming an end user is paid a mere \$10/hr) result in \$430 worth of losses, per year, per employee. So in a company consisting of 30 employees, that's \$12,900/year in losses. Finally, considering that Managed Services for 30 devices costs only \$8,160/year, having managed services not only pays for itself here, with this company, it also saves this company \$4,740/annually, just in this one regard alone. Plus, under Managed Services, preventative maintenance tasks are performed weekly, instead of monthly as with the traditional manual approach to preventative maintenance. Furthermore, performance analysis is more precise, because systems can be analyzed while they are in use (something that cannot be done when you're manually performing preventative maintenance, as you would obviously have to kick a user off their system to perform preventative maintenance tasks and analyze system performance). Finally, some tasks SHOULD be performed weekly, versus monthly, to ensure security and recovery capabilities, such as checking antivirus logs, performing weekly patching, and reviewing system backups. Under the traditional approach to preventative maintenance, this would result in additional costs for preventative maintenance, or under a preventative maintenance contract. This is not the case, however, under our Managed Services offering.

- 7. Faster Response Times When Remediation is Needed** – When issues do arise, obviously, the faster that you can respond to those issues, the faster they can be resolved (this is true in most cases – obviously there are always exceptions to that rule, however, like when hardware must be ordered and shipped from a supplier), and the less of an impact (financially- and productivity-wise) an issue has on the company. Due to the various different forms of remote access utilities included in our managed services platform, remote access is not a problem. Not only that, unless a company's Internet connection is being hindered in some regard (i.e.; by latency, packet loss, or over-subscription), remote access can often be established in as little as 10-30 seconds. These connection times rival alternative forms of remote access, such as Citrix GoToAssist, for example, which can take as long as 15-minutes to establish a remote access connection with an end user in need of IT Support. So if we round things off, and say that Managed Services takes on average 1 minute to connect to a remote system, it is in essence saving 14 minutes of billable support time, per remote access session

utilized. Hence, at a rate of \$85/hr for Field Service Engineer-level support, a company saves nearly \$20 per remote access session initiated by an IT Provider trying to provide support to said company. So if on average, a company is provided support remotely by their IT Provider 30 times each year, with Managed Services, that company saves \$600/year on those remote support sessions.

8. **Trend Forecasting for Planned Maintenance Windows** – As has already been touched on, the sooner you know about an issue, the sooner you can address it. Well, with our Managed Services offering, not only do we know about system resource shortages in general, but we can also predict them in advance. Our solution's ability to perform trend forecasting calculations enables our product to see in advance when additional system resources will be needed, by analyzing the average increase in resource utilization, on a monthly basis. In fact, as part of our managed services offering, we run quarterly trend forecasting analysis, for all of our customers, so that we can determine ahead of time when: (a) more memory will need to be purchased and implemented, (b) when additional hard drives will need to be purchased and implemented, or (c) when migrations to larger drives will be needed, (d) when additional CPU resources will need to be allocated to a VM, or (e) when a server will need to be upgraded (in the case of physical servers where no additional CPU sockets exist from which to allocate more CPU resources). The point here, however, is that by having a few months worth of advanced notice, a company can: (1) take their time and thoroughly research a replacement system, when needed, (2) shop around for the best price on upgrades or replacement systems, (3) schedule a planned maintenance window for upgrades or migrations, so that company productivity is not affected, and (4) save on shipping and handling (i.e.; by not having to make a panic purchase that requires overnight shipping).
9. **Remediation After Hours** – Another benefit of our Managed Services offering is that it provides 24x7x365 visibility for a company's network. Hence, as issues arise, they can be remediated, especially when they occur outside of normal business hours. For example, if an issue springs up overnight that will ultimately affect productivity the next business day, a business owner might very well desire to have the issue resolved before the next business day starts, in an attempt to prevent a loss of productivity on the part of his/her employees. While some business owners might cringe at the idea of paying after-hours support rates, in reality, it is often cheaper to address issues after hours, versus during normal business hours. For example, if an issue is identified (i.e.; one that will affect user productivity) at 1AM, and takes 4 hours to remediate, at normal Field Service Engineer-level support rates (and at time-and-a-half), the resulting billable charge would equal \$510.00. However, if the company pays an average wage of \$10/hr per employee, and has 30 employees, the same support delivered during normal business hours will cost \$1,540.00 (\$340 in billable support time, and \$1,200 in lost productivity). Hence in this example, it ends up costing the company \$1,030 more, by NOT having Managed Services. Therefore, without Managed Services, a company "Misses" 24x7x365 visibility for their networks, allowing both the identification of, and remediation of, critical issues during hours when company productivity will be affected the least. And, while not every

issue will affect a company's productivity, is it not better to at least have the option to choose to address issues when they will least impact your business?

10. **Behind the Scenes Remediation** – Another way in which our Managed Services offering saves a company money, is found in the remote access utility RSM (Remote Support Manager). This utility, which is packed full of various diagnostic tools, allows for remote access and remote remediation, both behind the scenes, and without affecting end user productivity in more than 80% of all cases (this is made possible by the fact that this utility prevents an IT Provider from having to remote control the end user's system in order to perform diagnostics and/or troubleshooting). Hence, using the same example of a business where the average employee is paid \$10/hr, and where over the course of the year 30 remote support sessions are required at an hour a piece to support a company's network, having the ability to perform behind the scenes remediation brings a company's productivity LOSSES down from \$300, to a mere \$60. This number obviously increases exponentially, as the number of remote support sessions delivered by an IT Provider, to a company, increases.