The DynaSis Education Series for C-Level Executives

Managed IT Security

Not very long ago, Managed IT Security was often considered an “add-on” to the other services a Managed IT Support Provider (MSP) would offer its clients. The MSP’s primary functions were making sure the network was installed and operating properly, along with updating software, applying patches, and repairing PCs and servers. Security meant installing and maintaining a firewall, as well as anti-virus software. More recently, however, several rather fast moving developments to the cyber crime landscape have moved IT security from being a small, though important part of the picture, to becoming a primary focus in protecting not only a business’ assets, but the very existence of the business itself.

Early cyber criminals had a difficult task. They had no one leading the way, explaining how to commit cybercrimes. If they wanted to hack a business’ records, they had to figure out how to do it by themselves. While there were certainly a number of brilliant, if misguided, minds that worked hard and accomplished these nefarious goals, it was not something open to the “masses.” When they did figure how to break through, they generally attacked large companies, which, never before having had to deal with these problems, were unequipped to defend themselves. Over time, however, these target companies fought back, spending great sums of money to institute defenses to keep the intruders out.

Fast forward just a few years and two developments have changed the scenario:

> 1: Most large companies have now spent great sums of money protecting themselves from cyber threats so that the average cybercriminal can no longer easily hack these companies’ networks. Because of this, cybercriminals have determined that the better target is the small business. It is easier to hack into the networks of dozens of unsuspecting small businesses than one large company, such as Sony or Target. Not only that, if they are really good at what they do, by hacking into the network of a smaller company that does business with a larger one, they might even be able to use that access to

slither their way into a larger company's network. That's exactly what happened with the Home Depot break in. The network of one of Home Depot's suppliers was hacked and the intruders were able to work their way into Home Depot's network from there, causing a lot of damage.

2: Let's say you want a spreadsheet program for your business. You have two choices: A) sit down at your computer for the next year and design and build one yourself from scratch, assuming you had the requisite years of training behind you, or, 2) buy a copy of Microsoft Excel for a few bucks. Well, that's exactly what has happened in the burgeoning cybercrime business.

Today, just like you can buy a complete suite of Office software from Microsoft, you can buy all the tools you need to hack into the network (and all the files) of unsuspecting businesses. You can then steal their information, and/or make changes to their records, and/or encrypt their files and hold them for ransom, and/or reveal private information to the public, or do whatever else your evil imagination dreams up. Yes, you can go online and for very few dollars buy all the software you need to become a very successful cybercriminal. Of course, the downside is a very long prison term when you are caught. The FBI tends to frown on such activities. (If you would like to learn more about this subject, we suggest reading our earlier White Paper, Cyber Security 2016.)

One of the techniques that the good guys use to thwart the bad guys and stay one step ahead of them is actually trying to hack into advanced systems themselves, thereby uncovering weaknesses or flaws and then fixing them. The April 8th edition of Security Week's online magazine (www.SecurityWeek.com) summarizes a paper produced by Columbia University researchers who attempted to, and succeeded, in breaking the "Captcha" systems used by Google and Facebook. Exactly what they did to break in, how successful they were at each level, and the suggestions they make for remedying the situations are outside the scope of this paper, but make interesting reading if you would like to go a bit deeper.

If you are the owner of, or an executive in, a small to midsized business and you have not been hacked, have not had your files encrypted (completely locked down until a ransom has been paid) and you have also not taken the requisite steps to prevent such actions, I am very comfortable in saying that your time is coming. Even those companies who have employed full-time IT staffs of one or more people are at risk unless those people have been given the tools they need. The easiest way to provide them with the tools, and often the most cost-effective, is to retain the services of a Managed IT Support Provider that takes an ongoing pro-active approach to cyber security. That said, it is important to understand that not all MSPs provide the same services or are as capable as each other. Some lead the way; others follow. Those that follow may be months behind in the technology of cyber defense, and in today's world, being months behind is roughly the equivalent of being in the stone-age.

Depending on the size of your company, the sophistication of your IT staff if you have one, your budget, the damage that can be done if your data is stolen or your system locked, and the importance of your system being "up" almost 100% of the time, there are a number of solutions that may work for you. (By the way, 99% uptime is not "almost 100%." In today's environment, 99.999% uptime equates to "almost 100%.")

If you are considering using an MSP, then consider this: On a very simplistic level, MSPs can be divided into two categories. On one hand there are the "break and fix" guys, and on the other, those that believe in preventing problems whenever possible, and immediately addressing issues when they do appear so as to prevent ongoing and extensive damage…true managed IT support providers.

In the "break and fix" scenario, your servers and work stations are running ok at any given time, but when something goes wrong or "breaks", you call your "computer guy" to come and "fix" it. The more things break, the more they need to be fixed. The more your employees are unable to work, the less service you can provide your customers, the more you spend on repairs, and the more money your computer guy makes.

The true MSP often works on a fixed monthly fee. For this fee they will guarantee your system will be up and running with a certain minimum annual downtime. Because they are responsible for your system and all its components, including all your workstations, servers, firewalls, etc., the better the quality of service they provide, the fewer problems you have, the fewer service calls that are required, the more money they make. Instead of your financial benefits being at cross-purposes as with the "break and fix" model, you and your MSP both come out ahead when there are fewer problems and minimized downtimes. While on the surface, switching from break and fix to MSP may seem like an expensive proposition, it almost always results in a cost-neutral to a money saving event for the client.

Here is another way to look at this: is your provider (or your in-house team) treating symptoms or fixing the problems. In another Security Week article, Joshua Goldberg states that he is dismayed to discover that most organizations chase symptoms rather than fixing the root causes. Frankly, we don't find that surprising because few small to mid-sized businesses have the teams nor tools necessary to pro-actively root out the causes of problems and, therefore, are always scrambling to fix these problems as they surface. Also not surprising is the reality that many companies that need and can afford the services of a highly competent MSP never even look into hiring one because their in-house team (often one person) feels threatened and convinces the owner/CEO that such a service is unnecessary. But here is the reality:

It is all but impossible for a small to mid-sized business, on its own, to provide itself a level of security that even minimally approaches the level that can be provided by the right MSP. Not only that, in the long run, they probably are not even saving themselves any money! That might sound self-serving on our part, but cyber security has become a highly specialized and constantly changed field. By the time your in-house person has become aware of the newest threats and made the changes necessary to combat them, even newer threats have emerged. A good MSP has teams on duty around the clock, constantly monitoring your system and installing critical updates and patches as soon as they become available, and, if an intrusion occurs at any time, including at 4 AM on a Sunday morning, has the ability to lock down the system to keep damage to a minimum.

A variety of MSP security "solutions" are listed below. These "solutions" all assume a high level of competence provided by your MSP.

> **Monitoring only:** At a minimum, any company that considers itself at risk of cyber attack or equipment failure (and who isn't?) needs to engage a company that offers 24 / 7 / 365 monitoring and that can sound the alarm at the first hint of a problem. The provider should also suggest in advance your options as to how you will handle events if and when they happen.
>
> **On-Site, using your own equipment:** Your equipment remains located in your facility, using the expertise of the MSP. This is the basic "full-service" model and is dependent upon the MSP inspecting your facility and your equipment and determining that the equipment is still fully functional and, if given the routine maintenance that the MSP will provide, will require little if any ongoing emergency

repair work. In the alternative, if it is determined that the equipment does not meet these standards, your MSP may offer limited repair services with options for additional work as needed.

On-site, with the MSP provided equipment: Although this may sound like an expensive alternative, it rarely is. The MSP has several advantages: first, it can purchase the equipment at a far better price than the typical SMB. Secondly and more importantly, because the MSP is going to provide ongoing routine maintenance for this new equipment, it knows that little emergency service will be required, plus it also knows that the equipment will last far longer than it would in a typical office setting. It also behooves the MSP to provide high-quality equipment, much to the benefit of the client. Compare it to a typical automobile versus a commercial airliner. Very few of us give our cars much maintenance beyond that required by the manufacturer, but airplanes, for obvious reasons, are given routine inspections and tests after every flight. Today's average automobiles are scrapped after 200,000 miles but it has been estimated that if they were given the same care as the typical jetliner, they would be on the road for more than 1,000,000 miles.

Off-site, with MSP provided equipment: This is what is known as "The Cloud". Your data and applications are stored in the MSPs highly secure data facility. This is the ultimate step up, providing the maximum in security, availability (goal 99.999% uptime) and mobility (company data and applications safely available to your team anytime, anywhere.) (If you would like to learn more about the Cloud, see our white paper: "Top 3 Reasons to Move to the Cloud".)

Hybrid systems: A truly flexible MSP will work with you to figure out what is the best approach for your business. While the four solutions above may seem to be flexible enough in and of themselves, your best solution may be a hybrid that takes a piece from one and a piece from another. Your MSP should never use a cookie-cutter approach. As an aside, some of the really large MSPs that have hit the market recently are not necessarily known for their flexibility or for taking the time to customize solutions for their clients. Nor are you likely to be working with the same support technicians.

While making the decision to work with a Managed IT Support Provider may seem like taking a giant step into the unknown, and that you may be giving up a comforting level of control over your network, what you will be accomplishing will actually be more control over the positive outcomes you should expect from IT, security of your network and data, and the mobility to allow your employees to safely and easily work from the office, home, the local Starbucks, or anywhere in the world.

1: https://en.wikipedia.org/wiki/Managed_security_service

2: DynaSis White Paper: Cyber Security 2016

3: http://www.securityweek.com/

4: http://www.cs.columbia.edu/~polakis/papers/sivakorn_eurosp16.pdf

5: http://www.securityweek.com/your-security-team-treating-symptoms-rather-problems

6: DynaSis White Paper: Top 3 reasons to Move to the Cloud