SWK TECHNOLOGIES

White Paper

Why Price is the Wrong Criteria When Choosing an MSP

By: Kevin Snyder

VP, Network Services

SWK Technologies

120 Eagle Rock Ave, Suite 330 • East Hanover, NJ 07936
Phone: 973.758.6100 • Fax: 973.758.6120
www.swknetworkservices.com

Table of Contents

Introduction

This white paper describes the rapid worldwide growth in cybercrime and the various measures your Managed Service Provider (MSP) should take to minimize your organization's risk. It also makes clear that, given this rapidly evolving cyber environment, price can be the wrong decision criteria to use when evaluating an MSP's IT services. The old adage that "you get what you pay for" is often true.

By definition, a Managed Service Provider is an outsourced IT partner who manages the productivity, reliability and vulnerability of its clients' computers, networks, and data. A qualified MSP will implement a toolset that is consistently reengineered to minimize risks to these vital assets. This is a measured, proactive, full-time endeavor. Today's managed service support plans are often available at flat monthly fees.

The Explosion in Cybercrime

Cybercrime is crime committed using computers, the Internet or technology in general. Data theft, fraud, and stalking are common, and neither the smallest nor largest of organizations are excluded from this crime wave. Cybercrime has evolved from a highly targeted approach to a random search of IP addresses. That means everyone is susceptible – individuals and businesses of all sizes!

In fact, the last five years have shown a steady increase in attacks targeting businesses with fewer than 250 employees, climbing from 18% to an astounding 43%. *-Symantec*

While cybercrime cost businesses an estimated $100 billion in 2013, and skyrocketed to $500 billion in 2015, analysts are predicting that the cost of cybercrime will reach $2 trillion dollars by 2019. *–Forbes*

According to International Data Group (IDG), 38% more cybersecurity events occurred last year compared to the year prior, while another study showed that 48% of data breaches occurred as a result of malicious intent. The remaining were related to system failure and human error!

Types of Cybercrime

Common forms of cybercrime in business include:

Identity Theft: In today's world of online shopping, banking and business, identity theft is the practice of robbing, and/or misusing another's personal information to steal or benefit from these activities. This information may include logon credentials, social security numbers, and credit card numbers.

Phishing: An attempt to deceive others to unknowingly reveal personal information. Phishing is most often seen in the form of emails that appear to come from trustworthy businesses or entities, but are malicious fakes.

Hacking: In the case of hacking, computers and networks are broken into, to steal personal, private, and valuable data of all sorts. Hackers often use sophisticated software to take advantage of weaknesses in computer operating systems, software, and security systems. The rightful owners of this valuable data often are unaware that this is happening.

Denial of Service (DoS): These attacks are designed to make networks and Internet resources or services inaccessible. This is accomplished by flooding the resource with such a tremendous number of requests that it's overburdened and rendered useless.

Malicious Software: We commonly see such software in the form of viruses and malware that may be intended to steal data or damage software programs. Ransomware has become an extremely prevalent form of malicious software that's designed to block access to computers and data until a ransom is paid, if not permanently.

Recent Local and National Occurrences

- In 2016, a medical diagnostics company in the northeast reported that hackers obtained information on approximately 34,000 individuals. That information included names, birth dates, lab results, and in some cases, telephone numbers. *–ABC News*
- The mayor of Plainfield, NJ reported hackers had demanded money in exchange for encrypted files because of a ransomware virus. Investigators found that the virus had entered through a computer in the finance department. *–NJ 101.5 News*
- The small village of Ilion, NY made ransom payments after two official looking emails released a virus throughout its system, causing software damage. The comptroller's office said the experience should warn others of the growing threat, which can infiltrate computers and make them inaccessible. *–NBC News*

On a larger scale:

- A hacker posted LinkedIn data on the Internet for sale, which allegedly included user names, passwords, and email addresses from 167 million LinkedIn accounts. *-Fortune*
- The Internal Revenue Service, at the height of the tax season, announced a massive breach exposing information of more than 700,000 individuals including Social Security numbers, birth dates, and other personal information. *–USA Today*
- Even the US Federal Bureau of Investigation, Department of Homeland Security had the records of 30,000 FBI and Homeland Security workers exposed including names, titles and contact information. Worse, the hacker claims to have even more files, totaling 200 Gigabytes! *-CRN*

Today's Businesses and Data Are Vulnerable

Everyday tasks like checking email and browsing the web expose your computer and network to vulnerabilities through viruses, spying, data theft, and software damage. Untrained employees often miss the red flags that may have prevented disasters.

Computers that lack the basics of operating system updates, antivirus and anti-malware software are open invitations for malicious destruction. Many employees connect to corporate networks utilizing personal laptops, tablets, and phones that fail to meet the security standards of the company, which multiplies the threat.

Weak computer account and password policies provide easy access to the malicious intention of intruders and even disgruntled employees. Consider the threat of employees who possess the freedom to download and install remote access programs for afterhours access to copy, share or damage the company's most precious data.

Well-intended employees make mistakes, too. While file sharing programs are commonplace in businesses today, productive employees who install them without authorization, in effect, send company data home to personal computers and devices.

Meanwhile, wireless networks have taken vulnerability to a new level. Passwords are commonly shared with employees, guests, and customers, allowing each device's malware to run rampant among all computers on the network.

And, it's not only technology we have to worry about. Are your confidential computers securely locked away? Are your outside vendors screened? How about natural disasters, including fires, floods, and earthquakes? The list goes on and on.

So, What Do You Have To Risk?

Many businesses tend to think broadly about risk, generally concentrating on the concerns and expense of downtime, but let's take a closer look. In the event of a cyber-attack, product and service delivery issues may immediately come to light. Before long, customer satisfaction is at risk, while employee morale suffers. Even payroll is in jeopardy. Lawsuits often result, and penalties are abundant in regulated industries such as health care, insurance, title, and law. Additionally, businesses that accept credit cards risk breaching PCI compliance regulations.

Damaged reputation throughout the industry, community, and among peers may result as well.

The bottom line, The U.S' National Cyber Security Alliance found that 60 percent of small companies are unable to sustain their businesses over six months after a major cyber-attack.

Your Managed Service Provider's Strategy

It's clear that Managed Service Providers have a significant task in keeping your network productive and secure. You'll want to select an MSP with a clear strategy and the bandwidth, both from financial and personnel skill base perspectives, to see that strategy through. Businesses most often replace their MSP's because they simply are not responsive. Yours must be, and must provide full-time helpdesk and onsite services.

Search for one that's not only large enough to support their existing customers *and* you, but also one that has achieved extensive industry certifications in the realm of network design and security. If your computers run Windows servers and workstations, your MSP should be Microsoft certified. Firewalls, virtualization, wireless networking, business continuity and disaster recovery, all certified!

In today's environment, it's no longer wise to interact with your IT provider only when something seems to be broken. That's too late. The right managed service provider will monitor your network around the clock, so trouble signs are detected and issues eliminated before they escalate into serious problems. Key considerations should include:

1) The MSP must have a plan to protect your business. The best will deploy a refined software suite to standardize every computer on your network. Each one will be protected by the same automated updates, antivirus software, and anti-malware software; and certainly, web filtering to thwart malicious attempts to steer employees toward infected websites.
2) Implement an Internet Use Policy, along with your MSP, to outline appropriate use of the Internet, email, and chat. Have a Remote Access Policy to share acceptable methods to access the internal network from remote locations, and a BYOD (bring your own device) policy that covers any acceptance of personal devices on your network, their usage, and any prior requirements.

3) Schedule periodic network risk assessments for your internal network and vulnerability scans that test the security of your inside internal from external threats.
4) Seek cyber liability insurance that covers expenses such as lost revenue, reputation management, and investigation in the case of a cyber-attack.
5) Finally, recognize that none of these is powerful enough to protect your network from human error. Request training from your managed service provider to minimize costly employee mistakes.

Final Words: Be Fearful of MSP's who say they can Lower Your Bill

Given the cyber environment in which we now live, and the complexities of defending your business, price is the wrong decision criteria to use when evaluating a managed service provider. That is not to say that price should not be a consideration. But if price is your key decision criteria, you may put your business in harm's way.

A low price often indicates that the IT provider is using a less sophisticated or an incomplete toolset. Likely, they haven't invested in the personnel, education, process, and tools to properly protect your network and data.

With the right MSP, your savings come soon enough. Your goal is to find a partner who has a history of lowering IT costs over time by increasing the productivity of their clients' networks. As an MSP solidifies and matures your infrastructure, the labor requirements of managing that network will go down, as should your monthly bills. The worse shape your infrastructure is in at the starting point, the longer-term perspective you must take to price efficiency. Instead, focus on finding the right partner; a partner who has a demonstrated history of perfecting and securing their client's networks and passing on the resulting cost savings to its client's over time.

About the Author

Kevin Snyder is the Vice President of Business Development for the Network Services division of SWK Technologies, Inc. Prior to joining SWK, Kevin was co-owner of Productive Tech, Inc., a privately-held Managed Services Provider located in Westville, NJ. In 2015, Productive Tech was acquired by SWK Technologies. Kevin's background includes a 20-year career as an entrepreneur, a technologist, and business consultant.

About SWK Technologies

SWK Technologies is a wholly-owned subsidiary of SilverSun Technologies Inc. (NASDAQ: SSNT). SWK's Network Services is ranked #45 globally by MSPmentor 501 in 2016 and was selected by MSPmentor 501 to receive the 2016 Vanguard Award as the most innovative MSP among the top 500. SWK is also a member of the CRN Solution Provider 500.

Partners include Microsoft, HP, Dell, SonicWALL, VMware, Cisco, Aruba, Symantec, Webroot, APC, Datto, and numerous others. SWK is proud to serve on the boards and advisory councils of several world-class technology and security organizations.