Basic PC Fixes costing you money

When your employees seek your IT security staff's help to fix their personal computer problems, it's often perceived as a productive use of everyone's time. After all, employees must have working computers and IT professionals are expected to resolve any technology issues. What doesn't get acknowledged however, is that instead of troubleshooting technical problems, your technology support staff could be spending their time on more productive tasks.

Cost of Fixes

According to a survey of technology professionals, companies waste as much as $88,660 of their yearly IT budget as a result of having security staff spend an hour or more per week fixing colleagues' personal computers. The 'wasted amount' was based on an average hourly salary of IT staff multiplied by 52 weeks a year. Other than knowing how much time is wasted, what makes things worse is that IT security staff are among the highest paid employees in most companies.

The fixes have mostly to do with individual rather than department or company-wide computer problems that don't necessarily benefit the entire company. The resulting amount is especially staggering for small and medium sized businesses whose limited resources are better off spent on business intelligence tools and other network security upgrades.

Other Costs

All those hours spent on fixing personal computers often means neglecting security improvements. The recent WannaCry ransomware attacks, which successfully infected 300,000 computers in 150 countries, demonstrate the dangers of falling to update operating system security patches on time. It should be a routine network security task that, if ignored, can leave your business helpless in the face of a cyber attack as formidable as WannaCry. It didn't make much money, but had it been executed better, its effects would have been more devastating to businesses, regardless of size.

Profitable projects could also be set aside because of employees' PC issues. For SMBs with one or two IT staff, this is especially detrimental to productivity and growth. They can easily increase their IT budgets, but if employees' negligible computer issues keep occurring and systems keep crashing, hiring extra IT personnel won't do much good.

What Businesses should do

The key takeaway in all this is: Proactive IT management eliminates the expenditure required to fix problematic computers. Bolstering your IT infrastructure against disruptive crashes is the first step in avoiding the wasteful use of your staff's time and your company's money.

Even if your small business has the resources to hire extra staff, the general shortage of cyber security skills also poses a problem. Ultimately, the solution shouldn't always have to be increasing manpower, but rather maximizing existing resources.

Having experts proactively maintain your IT eliminates the need to solve recurring small issues and lets your staff find a better use for technology resources. If you need non-disruptive technology call us today for advice.

E-SAFE TECHNOLOGIES

July 2017

In this issue…

HHS warns of fresh WannaCry-like attacks after Microsoft, DHS reports

The U.S. Department of Health and Human Services issued a security alert to healthcare organizations on Thursday, warning of recently discovered Windows vulnerabilities and a new threat with WannaCry-like capabilities.

The alert is a response to two reports released last week by Microsoft and U.S. Department of Homeland Security.

DHS and FBI alerted to a threat called Hidden Cobra, which is targeting U.S. critical infrastructure, media, aerospace and financial sectors. Thus, HHS officials warned, “targeting of the healthcare and public health sector systems and devices in the U.S. is possible.”

The researchers found the IP addresses connected to a malware variant used to manage North Korea’s DDoS botnet infrastructure. The malicious activity dubbed Hidden Cobra covers all malicious North Korean cyber activity that include DDoS botnets, keyloggers, remote access tools and wiper malware.

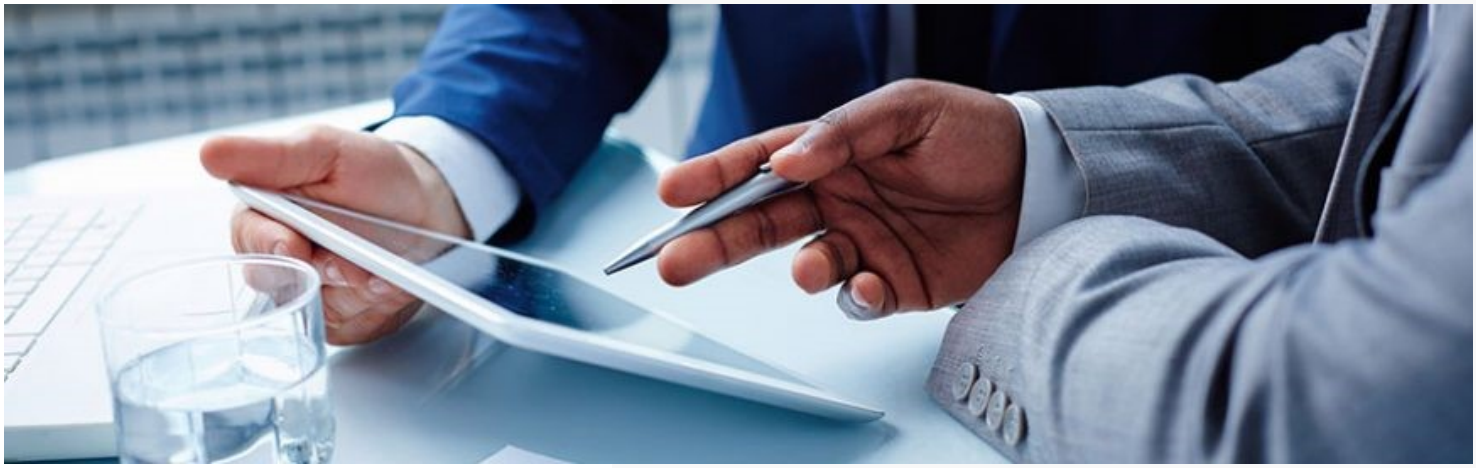
Hidden Cobra has been in place since 2009 and commonly targets older, outdated and unsupported Microsoft operating systems. The most recent threat highlights the DDoS tool capable of launching DNS attacks, Network Time Protocol attacks and Character Generation protocol attacks.The malware operates on victims’ systems as a svchost-based service and can download executables, change its own configuration, update its binary, terminate its process and both activate and terminate DDoS attacks.

Microsoft made an unprecedented release of three patches last week for vulnerabilities in XP and Server 2003 that could leverage SMB flaws like those used in WannaCry. Two other vulnerabilities allow malicious code to spread through shared drives and networks.

The company said it hopes to combat potential nation-state activity and destructive cyberattacks like WannaCry and Hidden Cobra viruses with its release. However, in its warning, HHS said these patches won’t necessarily protect against Hidden Cobra, as it leverages a wide range of vulnerabilities.

“These vulnerabilities allow an attacker to remotely run programs or attacks on systems,” officials said. “This could allow an attacker to perform a wide range of actions including exfiltrating documents or data, or gain access to other internal systems via the local network once initial access is gained.”

-Story by Jessie Davis from HealthCare IT News



The benefits of virtualization in 2017

The relationship between computer hardware and software can be frustrating. Both require the other to function properly, but both also require individual attention. Virtualization makes this relationship far more flexible, and we've got a rundown on a few of the best examples.

More technology uptime

Virtualization vendors use lots of fancy names for the features of their technology, but behind all the technobabble are a number of revolutionary concepts. Take "fault tolerance" for example. When you use virtualization to pool multiple servers in such a way that they can be used as a single supercomputer, you can drastically increase uptime. If one of those servers goes down, the others continue working uninterrupted.

Another example of this is "live migrations," which is just a fancy way of saying that employee computers can be worked on by technicians while users are still using them.

Say you've built a bare-bones workstation (as a virtual machine on the server), but you need to upgrade its storage capacity. Virtualization solutions of today can do that without the need to disconnect the user and restart their computer.

Better disaster recovery

Data backups are much simpler in a virtualized environment. In a traditional system, you could create an "image" backup of your server -- complete with operating system, applications and system settings. But it could be restored to a computer only with the exact same hardware specifications.

With virtualization, images of your servers and workstations are much more uniform and can be restored to a wider array of computer hardware setups. This is far more convenient and much faster to restore compared to more traditional backups.

More secure applications

In an effort to increase security, IT technicians usually advocate isolating software and applications from each other. If malware is able to find a way into your system through a software security gap, you want to do everything in your power to keep it from spreading.

Virtualization can put your applications into quarantined spaces that are allowed to use only minimum system resources and storage, reducing the opportunities they have to wreak havoc on other components of the system.

Longer technology lifespans

The same features that quarantine applications can also create customized virtual spaces for old software. If your business needs a piece of software that won't work on modern operating systems, virtualization allows you to build a small-scale machine with everything the program needs to run. In that virtual space, the application will be more secure, use fewer resources, and remain quarantined from new programs.

Employee computers need only the hardware required to run the virtualization window, and the majority of the processing takes place on the server. Hardware requirements are much lower for employees and equipment can be used for several years.

Easier cloud migrations

There are several ways virtualization and cloud technology overlap. Both help users separate processing power from local hardware and software, delivering computing power over a local network or the internet. Because of these similarities, migrating to the cloud from a virtualized environment is a much simpler task.

There is no debate about the benefits of this technology. The only thing standing between your business and more affordable, efficient computing is an IT provider that can manage it for you. For unlimited technology support, virtualization or otherwise, on a flat monthly fee -- get in touch with us today!

How thin and zero clients save money

Businesses are always looking for ways to cut costs without sacrificing growth. For the longest time, many believed that they had to purchase workstations with its own processing power, RAM, and hard drive. But thanks to virtualization, companies can save money and get the computing processes they need with thin and zero clients.

What are thin and zero clients?

Thin clients are stripped-down computers with minimum processing power and memory. They rely on a basic operating system and a network connection to access a more powerful . system where almost all computing processes take place.

Zero clients work the same way. The only difference is that there's no local storage or operating system installed on the device; all the software, storage, and processing power sits on a server until you need it. This setup makes it ideal for cutting costs, and here's why.

Reduced hardware costs

When it comes to upfront costs, thin and zero clients are the obvious choice. Conventional desktops start at $300 per user, while thin clients can go for as low as $90 per user. And since they have no hard drive or other moving parts, lean devices tend to be more durable and have a longer lifespan than their traditional counterparts.

Simplified IT management

Another benefit of thin clients is that they can be managed from a server. Suppose a new software update was released. Instead of manually downloading the patch on each computer, you can simply install the update on your server and roll it out to all thin clients. Apart from upgrades, you can make backups, security configurations, and application deployments in the data center. This quickens setup, reduces downtime, and increases employee productivity.

Minimized security risks

Thin clients also help you avoid costly malware attacks and data breach incidents. Your employees and poorly managed endpoints are the biggest vulnerabilities with traditional desktops. Thin and zero clients reduce these problems by limiting direct access to the operating system. This prevents employees from copying sensitive data to removable media and installing software, malicious or otherwise.

If your thin client is damaged or corrupted, you don't have to worry about your data, as it's originally stored in an impenetrable server.

Decreased energy consumption

Because processing is done locally, traditional desktops generate a lot of heat and require more power, which results in huge power and cooling bills at the end of the month. By contrast, thin and zero clients consume only 4-6.5 watts of power, almost 1/50th of thick client requirements. What's more, they require little to no cooling, allowing you to enjoy significant cost savings.

When looking for cost-cutting solutions, thin and zero clients should never be overlooked. The reduced hardware costs, power bills, and security risks are just too good to pass up. But if you're still unsure about this technology, give us a call. We'll assess your tech needs and determine whether or not thin or zero clients can help you succeedseveral years.