January 2015

TechTidbit.com

brought to you by Tech Experts

Is My Business Data Safe in the Cloud?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

One of the newest business technologies is "the cloud" that more and more people are using. It's an elusive term that is difficult to pin down, and it is precisely that vagueness that inspires fear in those who are considering transferring sensitive business data to it.

The cloud, however, isn't as mystifying as you may think, and, if you use an online data drive or social media, you are already using it. Simply put, the cloud consists of networks of servers worldwide that are capable of storing information.

The primary benefit of using the cloud for business is that it eliminates the cost and hassle of purchasing and maintaining a physical server. Also, employees don't have to waste time downloading and running applications and programs when they can pluck what they need from the cloud and virtually put it back when they are done. While this all sounds well and good, the question remains, "Is business data safe in the cloud?"

The reality of the situation is that even the most sensitive business data, with the right security precautions, can be as safe in the cloud as it is on a company's physical server.

For one thing, in the cloud, information is stored between multiple servers. This means, if one of those servers goes down, your data is still out there and retrievable wherever you are.

It is like having a backup copy in case a computer crashes or equipment is stolen; you don't have to worry about losing your business data when you need it the most.

Once people can feel comfortable storing their information in an intangible abyss, there may be lingering fears about who else is capable of accessing your company's valuable data. Cloud-based services and programs are now giving extra attention to this potential threat and have greatly increased security measures. Aside from 24-hour monitoring and secured entry to facilities where individual servers are kept, there's more to protect your information.

All of your data is encrypted when it enters or leaves the cloud, and it is continually backed up as well. Your business also retain proprietorship over the data regardless of where it is stored, so there really is no reason not to try increasing your company's productivity and efficiency by using the cloud.

Is Budget A Good Metric For Security?

Michael Menor is Vice President of Support Services for Tech Experts.

Is budget a good metric for security? In other words, if an organization wishes to improve its security, is spending more money an appropriate response? Furthermore, how can an organization ensure that any additional budget it allocates to security is spent wisely?

Talking about an organization's security program in terms of its budget is something we are quite accustomed to. We often hear people discussing security spending in the context of evaluating an organization's security posture.

For example, it's not uncommon to hear statements such as "In an effort to improve its security, the organization has increased its security budget by 30%." Of course, it goes without saying that a sufficient budget is necessary to accomplish anything.

Additionally, and perhaps quite obviously, it is important to note that larger organizations will need larger budgets to achieve the same level of execution.

What seems to be missing from the discussion, however, is the answer to a slightly different question: Does the organization spend its budget effectively?

A proper budget is indeed necessary, but it's equally important how the budget is spent. Not every dollar spent will have the same impact on security posture.

Sometimes, we think about budget in a backwards manner. Oftentimes, clients say things like "I need a firewall," "I need an IDS," or "I need a DLP solution."

The security organization will then communicate the business' need for each of these requirements to the executives and make the case for the required budget accordingly.

If a new requirement arises down the line, the client will request more budget, which it may or may not receive.

The issue with this approach is that a security organization's respective security programs are not tasked with things like "buy a firewall."

Just purchasing a network firewall will not stop an attacker from walking into your organization and physically plugging his computer into your network.

Maintenance and having the proper security policies in place is as equally important as having the appropriate equipment.

Take a look at this perspective. You never buy a car just to drive it around aimlessly. It involves proper maintenance and there are always risks that need to be identified each time you're driving.

You need to mitigate, manage, and minimize risks and that's essentially what the security organization does. Those risks can then be broken down into realistic and attainable goals and priorities.

Once we look at that list of goals and priorities, we soon realize that we have a framework in which to build our security operations. It is into this framework that we can drop all of our operational requirements.

Each goal generates a set of operational requirements and these spell out the peoples, processes, and products required to meet that specific goal.

It's worth noting that each operational requirement may take one or more products to address. Similarly, each product may address one or more operational requirement.

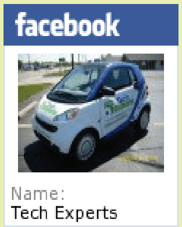
While keeping that in mind, it's possible to quickly build a matrix that will allow security organizations to map and optimize the products that best address the operational requirements.

It will take some time to transform budgetary discussions from product-centric to operation-centric.

However, as executives and boards see the direct correlation between increasing budget and improved security posture, they will be more likely to approve future budgetary increases.

So, getting back to the original question: Is budget a good metric for security? I would say that budget is not a metric at all, but rather a means to address operational security requirements.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

What You Need To Know About Network Security Devices

Scott Blake is a Senior Network Engineer with Tech Experts.

With cyber hacking, identity theft and malware programs on the rise, it's become even more important to protect your business networks from cyber invaders. One of the best ways to accomplish this is through the use of network security devices and installed anti-virus software.

Security devices attached to your network will act as a front line defense against threats. It behaves as an anti-virus and anti-spyware scanner and a firewall to block unauthorized network access.

It also acts as an Intrusion Prevention System (or IPS, which will identify rapidly spreading threats like zero day or zero hour attacks) and a Virtual Private Network (VPN), which allows secure access via remote connections.

Security devices come in four basic forms: Active, Passive, Preventative and Unified Threat Management (UTM). Active devices with properly configured firewalls and security rules will be able to block unwanted incoming and outgoing traffic on your network.

Passive devices act as a reporting tool that scans incoming and outgoing network traffic, utilizing IPS security measures. After reviewing these reports, the Active devices can be adjusted to close any detected security holes.

Finding and correcting possible security concerns is accomplished through the use of Preventative devices. These devices scan your network and identify potential security problems.

They will generate a detailed report showing which devices on your network need improved security measures.

UTM devices combine the features of Active, Passive and Preventive devices into one compact device. UTM-enabled devices are the most commonly found security device in small and medium-sized businesses.

By incorporating all the features into one device, your network administrator is able to more easily manage and maintain the security of your network. This greatly reduces overhead to your business.

Many businesses think they know what security measures need to be in place. Often, security professionals will find basic or home-class routers installed in companies.

While the upfront cost of the home-class router is lower than a business-class security device, the fact of the matter is that the home-class routers don't offer the features and security a business needs to protect their network.

Companies electing to use home based devices run a much higher risk of finding themselves the victims of cyber attacks.

Before purchasing any security device, it's best to consult with a security professional. Have penetration tests performed and a vulnerability assessment report generated.

The report coupled with the advice of the security professional will guide you in determining what device is best for your network and business.

The benefits to having a proper and professionally-installed security device in place include protection against business disruption, meeting mandatory regulatory compliances, and protection of your customers' data, which reduces the risk of legal action from data theft.

Along with the proper security device in place, you also want to make sure every device on your network is running a robust anti-virus program.

Managed anti-virus platforms are best for any business. Your network administrator can manage, update, scan and remove any threats found on any system attached to the network. This greatly reduces overhead and employee interruption.

For professional advice on security device installation, anti-virus solutions, or if you're interested in network penetration testing, call Tech Experts at (734) 457-5000.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Five Great Google Search Tips

If you have ever felt discouraged when trying to find something specific on the web but Google search lists a ton of sites that aren't relevant, you're not alone.

Try these handy tips to hone your search terms and help Google locate precisely the information you need:

Tabs

Sometimes, the most obvious things are the most overlooked, and tabs at the top of search results are no exception. Get closer to your desired results simply by clicking the tab that best describes what you want.

If you need a picture, for example, select Images, and you will see nothing but images. The same holds true for news and more.

Quotes

Word order is often crucial to finding the right information, but Google search doesn't naturally take this into account.

For example, you may want to locate information about the movie Simon Birch, but your search turns up results for a guy named Simon talking about birch trees. Simply put quotation marks around your term to search for a precise phrase.

Hyphens

There also may be words or phrases you wish to exclude from your search results. In this case, put a hyphen in front of the term to indicate you don't want to see information that contains that term.

For example, if you wish to learn about antique dolls but are not interested in Barbie dolls, input antique dolls -Barbie.

Colons to Search Specific Sites

If you need to restrict your search results to a specific site, add a colon followed by the site address after your search terms to let Google show results only from that particular website. When you want to read news about the ebola virus just on CNN, for example, type in ebola virus: cnn.com.

This is also useful to search your company's website. Simply use the word site, a colon, followed by your company's website address. This will display all pages Google has indexed from your website.

Related Sites Search

Sometimes, you want to discover similar sites to ones you already enjoy. Let's say you like the types of articles on Elephant Journal but have already read everything there. You can find new and similar reading material by searching related: elephantjournal.com.

Using Flash Drives? Encrypt Them

Flash drives are becoming an increasingly popular means for transferring files from one computer to another – especially now that they are capable of storing up to a whopping 256 GB. These handy devices are easy to tote because of their small physical size and are a no-brainer to use since they pop right in and out of a USB port. So, it's no surprise that employees may use flash drives to transfer work from the office to home. While this may initially sound like a run-of-the-mill activity, think about the ramifications of taking sensitive company data out of the building.

A variety of methods have been used to prevent employees from using flash drives due to the security risk it poses. While establishing policies for using removable data is good practice, it isn't necessarily effective, and it is virtually impossible to monitor if and how flash drives have been used. This has spurred some businesses to physically disable the USB ports on its computers by calking ports or using software to disable them. This certainly works, but it is possible to eliminate the security risk without damaging any equipment or putting restrictions on employees simply by encrypting the data on drives.

There are two main ways to encrypt flash drives in order to prevent prying eyes from viewing your important business information. The first is to use drives that are outfitted with encryption service. As such, there is no worry about training your staff how to encrypt files or a question on whether it's being done at all. Encryption, however, can still be achieved on regular flash drives that may already be in employees' possession with software-based encryption services, most of which are low-cost.

In either case, sensitive business data that is encrypted is secure without a lot of hassle. When your employees need to access such files from flash drives outside of the office, they will be prompted to enter a password or encryption key to view them.

If a flash drive falls into the wrong hands, the information stored is completely unreadable without the proper key or password. This prevents any data breach while still allowing employees the ease of using flash drives to relay their work between the home and office.