October 2019

TechTidbit.com

brought to you by Tech Experts

Data Breaches Cost Healthcare $6.5M Or $429 Per Patient Record

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

Data breach costs are on the rise, with breach-related spending in the healthcare sector reaching $6.5 million on average, an IBM-sponsored report shows.

Data breaches cost the healthcare sector an average of $6.5 million per breach, over 60 percent more than all other business sectors, according to a Ponemon Institute report, sponsored by IBM. Other sectors spend about $3.9 million, on average.

Researchers interviewed 500 global organizations that experienced a data breach in the last year. The researchers found for the ninth consecutive year the healthcare sector is still the hardest hit financially by data breaches.

The costs are directly related to legal, technical, and regulatory functions, including patient notifications, breach detection and response, and lost business caused by reputational damage, loss of consumer trust, and downtime.

What's more, loss of business has remained the largest breach expense for the last five years among all industries, with a cost of $1.42 million, or 35 percent, on average.

The Ponemon report also showed some of these costs are also associated with the highly regulated nature of the healthcare sector, which can add to the financial impact. Healthcare had higher costs in the second and third years than other sectors.

About 67 percent of the costs occurred during the first year after a breach, 22 percent during the second, and 11 percent in the years that followed the two-year mark.

The researchers also found breach costs have increased 5 percent in healthcare in the past year. In fact, health providers will spend $429 per each lost or stolen record – up from $408 per record in 2018. The cost is about three times more per record than all other sectors.

Breach costs are rising across all sectors at 12 percent, with the impact lasting for several years after the initial incident, the report showed. The financial impact is directly related to increased regulation, the complexity of criminal cyberattack resolution, and the financial impact that can last for several years.

Further, the financial impact of breaches is twice as much in the US than other countries, at an average of $6.5 million. And those costs have increased 130 percent in the past 14 years. The average cost of a breach in the US was $3.5 million in 2006.

Those costs also varied by organization size, with small- to medium-sized organizations spending 5 percent of annual revenue, or $2.5 million to recover.

These numbers are especially concerning given a recent CHIME and KLAS report that found small providers are not keeping pace with necessary cybersecurity measures, like risk management, and governance.

Also concerning, malicious or criminal cyberattacks were behind 51 percent of all breaches and are the costliest in terms of recovery at 25 percent higher than breaches caused by system or insider error. These attacks have increased 21 percent from 2014 to 2019.

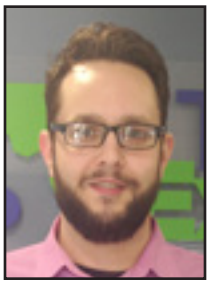
What's worse is that it took the breached US organizations an average of 245 days to identify and contain a breach. However, the report tied breach response directly to cost saving. Organizations that detected and contained the breach in less than 200 days spent $1.2 million less on total breach costs.

Lastly, organizations that focus on incident response can reduce the time it takes to respond and had a direct correlation to overall costs. Those that had these measures in place reduced their breach costs by $1.23 million, compared to those organizations without those functions.

Data breaches cost the healthcare sector an average of $6.5 million per breach, over 60 percent more than all other business sectors, according to a Ponemon Institute report, sponsored by IBM. Other sectors spend about $3.9 million, on average.

Has Windows 10 Deleted Your Programs?

"You upgrade to the latest version, go to use a program, and it's gone. While someone who works in IT will likely know what happened, the average user is in the dark. The same people Microsoft are "protecting" are left scratching their heads with no explanation."



Jason Cooley is Support Services Manager at Tech Experts.

With the litany of ongoing issues and quirks associated with Windows 10, we've come to expect hiccups but something is getting a lot of attention in the recent major upgrade patches.

Windows, silently and without notice, is deleting installed software.

While this can be infuriating, it is actually Microsoft attempting to look out for the average user. The belief is that the average user will not be able to deal with a program being non-functional, causing driver errors, or worse.

Although this makes sense, the issue isn't the fact that you are being protected. It's the lack of notification.

You upgrade to the latest version, go to use a program, and it's gone. While someone who works in IT will likely know what happened, the average user is in the dark. The same people Microsoft are "protecting" are left scratching their heads with no explanation.

Let's continue by acknowledging the fact that, even though these programs might have been uninstalled, the data associated with the program is likely safe.

Windows, during large feature updates, will create a Windows.old file. This will contain the previous version of Windows and the files associated with it.

The files that have seem to have vanished associated with your software? It's tucked away in the Windows.old folder.

However, do not assume this is a safe place to leave the data. If you need to have the data, make sure to copy it from that folder. After a week or two, it will be gone.

So is the folder there just to catch the programs and files Windows decided to remove? Nope! The good news is the main purpose of this folder is to store the version of Windows from before the large feature update.

This will allow you to roll back to the previous installation and use your software again. Your associated files would be back as well.

What's the catch? At some point, you are probably going to have to update. Windows is becoming increasingly strict about forcing updates to users at some point.

The good news is that a lot of the incompatibility issues will already be resolved by the time you're forced to update.

Granted, that's not guaranteed, so if you have essential software that may not be compatible moving forward, you would want to investigate other options.

This shouldn't be a problem for an average user. Normal everyday use programs like Microsoft Office will always be fixed when compatibility issues arise, assuming you are still using a supported version of the program as well. (Condolences to those of you still using Office 2007, but if it breaks, they aren't going to fix it.)

There are options to delay updates by default, which could possibly save you from ever having to deal with this problem.

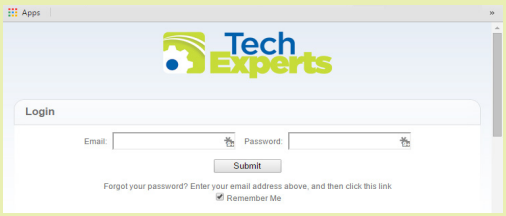
If you have to download programs to replace any outdated ones, be selective and make sure they're from reputable sources.

At the end of the day, Microsoft isn't trying to ruin your day, but some of these issues sure can do that, intentionally or not.

Give us a call if you have any questions about Windows 10 or application upgrades. We're happy to help!

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



Password Versus Passphrase... Which Is Best?

Passwords are something you use almost every day, from accessing your email or banking online to purchasing goods or accessing your smartphone.

However, passwords are also one of your weakest points; if someone learns or guesses your password they can access your accounts as you, allowing them to transfer your money, read your emails, or steal your identity. That is why strong passwords are essential to protecting yourself.

However, passwords have typically been confusing, hard to remember, and difficult to type. In this newsletter, you will learn how to create strong passwords, called passphrases, that are easy for you to remember and simple to type.

Passphrases

Passphrases are a simpler way to create and remember strong passwords.

The challenge we all face is that cyber attackers have developed sophisticated and effective methods to brute force (automated guessing) passwords. This means bad guys can compromise your passwords if they are weak or easy to guess.

An important step to protecting yourself is to use strong passwords. Typically, this is done by creating complex passwords; however, these can be hard to remember, confusing, and difficult to type.

Instead, we recommend you use passphrases-a series of random words or a sentence. The more characters your passphrase has, the stronger it is. The advantage is these are much easier to remember and type, but still hard for cyber attackers to hack.

Here are two different examples:
Sustain-Easily-Imprison
Time for tea at 1:23

What makes these passphrases so strong is not only are they long, but they use capital letters and symbols. (Remember, spaces and punctuation are symbols.) At the same time, these passphrases are also easy to remember and type.

You can make your passphrase even stronger if you want to by replacing letters with numbers or symbols, such as replacing the letter 'a' with the '@' symbol or the letter 'o' with the number zero.

If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

Using Passphrases Securely

You must also be careful how you use passphrases. Using a passphrase won't help if bad guys can easily steal or copy it.

Use a different passphrase for every account or device you have. For example, never use the same passphrase for your work or bank account that you use for your personal accounts, such as Facebook, YouTube, or Twitter. This way, if one of your accounts is hacked, your other accounts are still safe.

If you have too many passphrases to remember (which is very common), consider using a password manager.

This is a special program that securely stores all your passphrases for you. That way, the only passphrases you need to remember are the ones to your computer or device and the password manager program. Never share a passphrase or your strategy for creating them with anyone else, including coworkers or your supervisor. Remember, a passphrase is a secret; if anyone else knows your passphrase, it is no longer secure.

If you accidentally share a passphrase with someone else, or believe your passphrase may have been compromised or stolen, change it immediately. The only exception is if you want to share your key personal passphrases with a highly trusted family member in case of an emergency.

Do not use public computers, such as those at hotels or Internet cafes, to log in to your accounts. Since anyone can use these computers, they may be infected and capture all your keystrokes. Only log in to your accounts on trusted computers or mobile devices.

Be careful of websites that require you to answer personal questions. These questions are used if you forget your passphrase and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even on your Facebook page.

Make sure that if you answer personal questions you use only information that is not publicly available or fictitious information you have made up.

Can't remember all those answers to your security questions? Select a theme like a movie character and base your answers on that character. Another option is, once again, to use a password manager. Most of them also allow you to securely store this additional information.

Continued on page 4

"What makes these passphrases so strong is not only are they long, but they use capital letters and symbols. (Remember, spaces and punctuation are symbols.) At the same time, these passphrases are also easy to remember and type."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Are You Still Using Microsoft Windows Server 2008?

Microsoft will stop mainstream support for Server 2008 at the end of this year. This is a popular technology solution, so the end of support creates concern for many. Read on, and we'll explain what this means and what you should do.

What Does 2008 Server End of Life Mean For Your Company?

Windows Server 2008 end of life means that Microsoft will no longer update this product unless a warranty compels them to do so.

Unfortunately, many businesses are still not ready. The reasons vary, but many company owners stay busy running their day-to-day operations. They just don't have time for issues like this. And yet, this is a crucial server EOL that could cause many disruptions to your business if not dealt with promptly.

How Soon Should You Get A New Server?

You need to change over from the Windows 2008 Server and Windows 2008R2 to a supported server by the end of the year. That's the very last moment you'll have before support is no longer available.

Migrating all of your data, applications, and other IT solutions to new servers is a time-consuming and complicated process, so small businesses should not wait until the last minute.

By waiting, you place your technology assets in danger, and you could pay more for last-minute service. Think of this as an auto repair problem. The sooner you get it fixed, the less it will typically cost. Avoid extra costs and issues by upgrading your servers now.

What Other Problems Can Happen?

An end to bug fixes and those all-important security updates may be the ultimate deal breaker for you. Data managers will tell you that not having these fixes makes your data vulnerable to access by unauthorized parties.

Cybercriminals are on the look-out for ways to infiltrate your systems and steal sensitive data, and they know about the EOL for Windows Server 2008. Since Microsoft will no longer offer security updates and bug fixes for this server, this creates numerous loopholes in data security that could be exploited.

These security breaches can be avoided by installing a newer generation server with supported security updates.

What Should You Do?

There are many reliable servers available on the market today. This new generation of servers offers better efficiency, virtualization, faster speeds, and many other good attributes. Do some research to ensure that you get a proper replacement that will address all the functions that your organization requires.

How Do You Get Ready For The Upgrade?

Installing new servers can be challenging. You have to plan out the process so that everything is done correctly and during off hours, so it doesn't disrupt your daily operations. The sooner you start, the better.

To plan for an infrastructure upgrade, rewrite and migrate all applications based on Server 2008 to a safe storage place. The new server may require some troubleshooting. Databases can be hosted on the Windows Server 2008 hardware as you install the new system.

During the transition, put a data protection infrastructure in place that will eliminate risks during the server upgrade. This will protect your data from problems with the old server and risks associated with the new system. While this will cost extra, the fines associated with a data breach are often far more expensive.

Password Versus Passphrase... Which Is Best, continued

Many online accounts offer something called two-factor authentication, also known as two-step verification.

This is where you need more than just your passphrase to log in, such as a passcode sent to your smartphone. This option is much more secure than just a passphrase by itself. Whenever possible, always enable and use these stronger methods of authentication.

Mobile devices often require a PIN to protect access to them. Remember that a PIN is nothing more than another password. The longer your PIN is, the more secure it is. Many mobile devices allow you to change your PIN number to an actual passphrase or use a biometric, such as your fingerprint.

If you are no longer using an account, be sure to close, delete, or disable it. *(This article is reprinted with permission from the SANS Security Center OUCH! newsletter.)*