

## The Importance Of Confidentiality, Integrity, And Availability

Confidentiality, integrity, and availability. Without the proper balance of the business data triad, an organization would either be inefficient or extremely vulnerable. But why are these elements so important and how do you achieve them?

### Confidentiality

Confidentiality is about protecting information from disclosure to unauthorized users or groups. Information has value: bank statements, credit card numbers, trade secrets, and government documents. Everyone has information they wish to keep a secret.

A key component of protecting information confidentiality is encryption. Encryption ensures that only the authorized users can read the information being transmitted across local and wide area networks.

Encryption is an absolute must in today's digital environment and can be found in almost every major protocol in use by IT professionals. A very prominent example will be SSL/TLS, used in communications over the Internet. Other ways to ensure information confidentiality include enforcing file permissions and access control lists.

### Integrity

Integrity of information refers to protecting information from being modified by unauthorized individuals or groups. Information only has value if it is correct and tampering sabotages

that. For example, if you were sending an employee financially sensitive information, but the information was tampered with wildly inaccurate figures, the results of that could be very costly for your business.

As with data confidentiality, encryption plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the information of the original data must be provided to you in a secure fashion initially.

A much more convenient method employed by IT professionals include using existing schemes such as GPG, an encrypted privacy guard that digitally signs the data with a unique "digital signature" that cannot be replicated.

### Availability

Availability of information ensures that authorized parties are able to access the information when needed. In many ways, this is the most important aspect. Though, unfortunately, this usually ends up coming at the cost of confidentiality and integrity if not implemented correctly.

Information only has value if the right people can access it at the right times and denying access to information through DDoS attacks has become very common. The primary aim of


DDoS attacks is to deny users the resources of the website by flooding an organization's or website's network with traffic. The attacker will typically do this to the point of network failure. Such downtime can be very costly.

Other factors that could lead to lack of availability to important information may include accidents such as power outages, ISP outages, or natural disasters.

How does one ensure data availability? Backup is the key. Regularly doing onsite and/or off-site backups can limit the damage caused by attackers or unforeseeable events. Redundancy is an appropriate addition to regularly scheduled backups. Having an off-site location ready to immediately restore services to your primary data centers will heavily reduce the downtime in case anything happens.

The Business Data Triad is a very fundamental concept in information security and, at this point, there is no use "reinventing the wheel" on data security as it all still applies. Ensuring that the three facets of the "CIA" triad are protected is an important step in designing any secure system.

It can be overwhelming to the average business owner, but a managed service provider (MSP), such as Tech Experts, can provide an organization with the tools and policies needed to strike that perfect balance.



How does one ensure data availability? Backup is the key. Regularly doing onsite and/or off-site backups can limit the damage caused by attackers or unforeseeable events.

We're proud to partner with the computer industry's leading companies:



Microsoft Partner




Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.



## How The Internet Of Things Can Affect Your Business

*“Let’s say you have an Internet-connected thermostat. If someone was targeting you and gained access to your network, they can snoop around to see if there are places on your network where they can hide and wait for the right time to launch their attack on your system.”*



Ron Cochran is a Field Service Engineer at Tech Experts.

In today’s times, we all want to be connected to the Internet for ease of operation, but this could come with grave consequences. If you look around, you can find a smart version or a version of almost any device that’s able to connect to the Internet.

Kitchen appliances, lightbulbs, doors, air conditioners. These devices are part of a group known as The Internet of Things (or IoT, for short).

The Internet of Things is the internetworking of physical devices, vehicles, buildings, controllers, and sensors that all collect data, either for internal use or external use.

Now, you might think that is cool – and in most cases, it is pretty cool and convenient to be able to turn on your window air conditioner or ceiling fan with your phone.

At home, this poses very little threat to anything, although you might have a neighborhood kid that is learning how to crack a Wi-Fi password.

However, having these vulnerabilities at a place of business that

houses substantial personal or financial data becomes much more serious issue.

Right now, there are no mandates, laws, or regulations stating that the manufacturers of these smart devices or connected home adapters have to conform to a standard of encryption. The IoT is trying to put that in place to protect sensitive data.

Let’s say you have an Internet-connected thermostat. If someone was targeting you and gained access

You may think to yourself that your thermostat is receiving a software update. You’ll dismiss it as you’ll believe that’s supposed to happen.

In reality, the hackers are poking around, copying files, and stealing data.

Don’t think that nothing could happen from having an Internet-connected thermostat on your business network.

Hackers can and will find nooks and crannies to squeeze through to get to your valuable data.

Not to say that having Internet-connected devices around your home or business is a bad idea, but until proper regulations are set in place (and even after that), it would be a great idea to have all Internet-connected



devices isolated from your business network. You can isolate them by putting them on their own separate network by using firewall settings, different switches, and other settings.

If this is something that you think you might be interested in, we can help you with that solution. Either way, great caution should be used when adding these devices to your home or business.

Internet-connected devices can mine data without you even knowing it until it’s too late.



## Why Should You Keep Your Operating System Updated?



Jason Cooley is a Network Technician at Tech Experts.

Upgrading your operating system can be costly, especially for a business with a large number of users.

There's a good chance it's something that you will have to both plan and budget for.

While you may not "need" a new operating system to function day-to-day, what happens if you keep using your OS past the end of Microsoft support? What does end-of-support even mean?

These questions can easily be answered together. When Microsoft ends support for a product, they no longer provide automatic fixes, updates, or online technical assistance.

They also end all security updates that, during the normal life cycle of the operating system, fix any known security risks or issues.

So how are you more at risk?

If Microsoft stops applying updates, any new vulnerabilities discovered will remain that way, giving hackers and cyber criminals as much time as they need to discover any potential security issues that would allow them to infect your system, steal your personal information, or destroy your data, among other things.

Another issue with the end-of-support cycle is that cyber criminals can analyze the last security update. Using the information in the security update, they can discover what changes were made to close a known vulnerability.

That means cyber criminals now have the tools and information to reverse engineer the security fix and use it to create a loophole to get into your system.

Many companies have outdated versions of operating systems, but "sort of working" doesn't mean that it's still fine to use.

Many point-of-sale systems will still run on Windows XP and Windows XP has not been supported or updated in some time. These systems are substantial security risks.

Following the schedule of retirement, Microsoft recently ended all support for Windows Vista.

While general support ended in 2015, it became fully unsupported as of April 2017.

So many businesses use Windows 7 still and that too will go the way of XP and Vista.

A whole new system may cost the business a chunk of money, but consider the cost of lost data, a potential data breach of confidential or sensitive, data, or the loss of your system's functionality.

The list of repercussions could go on and on. Preventative upgrades will make you more secure and

allow you to plan for upgrades and changes, instead of working reactively when there is a problem.

Additionally, you can also evaluate cost if you upgrade preventively. Acting reactively will cause a scramble, potential loss of business, and force you into resolving the problem when it happens, even if it costs more than you are willing to pay.

At that point, what is there to do? You can't stop operating indefinitely while you sort out the details.

For Windows 7, Microsoft has announced that it will end support completely in 2020, so there is still plenty of time left to upgrade and transition smoothly, avoiding that scramble.

There are other things to keep in mind as well. While Windows 7 support ends completely in 2020, your support and updates may very well be over already if you don't update the service packs.

Make it a priority to ensure your business is regularly updating the system to keep it secure and up-to-date. Your system updates are always important, especially when it comes to security.

While there isn't a foolproof way to stay completely safe when using any device that connects to the Internet, start making the changes you can and plan accordingly.

You'll be much happier scheduling your upgrade than waiting until it is too late.

*"Many companies have outdated versions of operating systems, but 'sort of working' doesn't mean that it's still fine to use."*



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

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.



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](http://www.TechSupportRequest.com)



TECH  
EXPERTS

15347 South Dixie Highway  
Monroe, MI 48161  
Tel (734) 457-5000  
Fax (734) 457-4332  
info@MyTechExperts.com

## Equifax: A Nationwide Security Scare



*Evan Schendel is a help desk specialist at Tech Experts.*

How much is your personal information worth? Who would you trust with your most vital information? On September

7th, Equifax – the oldest of the three largest credit reporting agencies – notified the public of an information breach. This breach resulted in an estimated 143 million American’s personal data put at risk. While this number is staggering, what makes it even more daunting are a few specific items:

1. This nationwide breach occurred somewhere in the span of March to April of 2017. They reportedly discovered the incident at the tail-end of June, though sources differ on how long this has really been an issue. Regardless of the exact length, this is quite a long time to have any information at risk without knowing.
2. Three top executives at Equifax decided to sell approximately \$1.8 million worth of stock in their company in early August. Equifax stated that the executives had no knowledge of the breach at the time, but this doesn’t change how this looks in the eyes of the public.
3. Equifax’s credit protection site’s terms weave into the agreement that anyone who signs up for it waives their right to a class-action lawsuit against the company. Equifax

had released a statement noting that this agreement did not stand for the data breach and the agreement’s verbiage was changed to reflect this properly.

With these bits of information, half the nation seems doomed, but it’s not. There are ways to protect your credit and keep your money perfectly safe.

Equifax has set up a site – equifaxsecurity2017.com – with that same agreement noted earlier. This site will help in finding out if your information had been accessed. Regardless of your status on this site, precautions should always be taken.

Secure, difficult-to-guess passwords are always a good thing to have, but are sometimes quite tough to implement when you get down to it. A long string of letters and numbers that do not form words, typically 15 to 20 characters long, might be hard to recall and even more so when there are different passwords for every site you use.

Applications like Passport or LastPass can assist in this, keeping passwords safe and secure and ready to be accessed when you need them.

Make sure to monitor your credit if you’re notably at risk, keeping a keen eye on any accounts you might have. This doesn’t mean you need to hawk over a screen 24/7 – only that you’re alerted whenever something suspicious or odd occurs. You can then give the OK to place a stop on an account and prevent further transactions.

While this whole debacle may seem hopeless, it was reported that only 209,000 credit card numbers were touched, though it’s never good to turn a blind eye to financial security. If this does develop into a larger issue, the key to making sure your money is safe is responding to the issue quickly, to cut off the problem at the source.

After all, while this breach may be massive, it’s unlikely to have many effects on many people, at least for a while.

