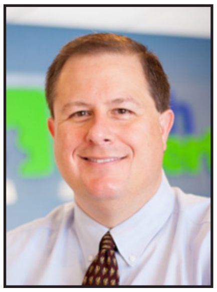
March 2022

TechTidbit.com

brought to you by Tech Experts

What Are The Five Perspectives In Business Analytics



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

Business analytics is an approach to identify the challenges faced by an organization and finding solutions to them. In other words, business analytics help you implement changes in the business to streamline tasks and activities.

Your role as business analysts is to bring efficiency to the working process. To analyze business activities and bring change, you need to understand how your business works. Depending on how it works, you need to consider the change you can bring to the organization to boost productivity.

Your role as business analysts is to bring efficiency to the working process. To analyze business activities and bring change, you need to understand how your business works. Depending on how it works, you need to consider the change you can bring to the organization to boost productivity.

Agile

Agility is an effective perspective to compare your traditional business analytics with new and advanced innovations.

The reason why this tool is effective is it provides you data considering your user stories and product backlog. Here are some benefits of using agility:

- Enables you to create user stories.
- Focuses on finding solutions analyzing the customers.
- Helps to stay in touch with the stakeholders and fill in the communication gaps.
- Provides tools to create documents such as wireframes and design flow.
- Enables you to review different stories and implement the business analytics process without violating business rules.

Business intelligence

This allows you to transform your data and produce actionable insights. It provides you software and other tools to develop tactics and strategies to make better decisions.

By using these tools, you can analyze and access new data and create summaries, graphs, reports, maps, and dashboards. All these reporting instruments will help you understand the settings in detail.

Information technology

Information technology supports your business by maximizing productivity and efficiency. It enables you to communicate with the teams and stakeholders and secure the data.

Today, all the business processes depend on information technology and tools. Here are some benefits of using information technology for business analytics:

- Streamlining communications
- Automating processes
- Securing the data
- Providing remote access and communication

Business architecture

Your business architecture can be elastic and scalable with big data.

Furthermore, you can understand the latest trends and demands in the market and enhance the business' architecture accordingly.

With the availability of cloud systems, you can perform business tasks at affordable rates.

Cloud technology scales up the efficiency of your development process and helps you design better prototypes.

Furthermore, this approach creates an amazing testing environment for data analysis.

Business process management

This approach helps you understand different operations and identify their health.

As a result, you can improve business process efficiency, offer a broader understanding of the management process and engage the teams to meet their goals.

To analyze your business successfully, you need to work on all levels and define new strategies to improve the business' architecture.

You should understand how to define goals, then improve the process through technology and supporting the teams.

Benefits Of Transforming Into A Paper-free Office

Going paperless at your office by digitalizing your documentation is a huge step.

Although it's not easy for many businesses to transfer the entirety of their paperwork electronically, you can start small and shift slowly. It involves numerous benefits, such as lower costs and higher efficiency after digitalization.

In a competitive market, cutting down on expenses and enhancing productivity is an arduous task. You can accomplish these tasks easily by going paperless.

The availability of advanced technological tools is making it easy to move your documentation online. If you are still confused about going paperless at your office, consider these benefits.

Better organization

Tracking and maintaining papers manually is a time-consuming task. Your employees may find it intimidating to handle all clutter and mess when it comes to documents. This becomes even tougher when you are running a large-scale operation. Paper documents increase the risk of huge errors and blunders.

Going paperless will streamline your management and organizing tasks so your employees can channel concentration towards high-priority tasks. This avoids tedious paper hunts. You will face a lower chance of human errors and mistakes by introducing coherence and proficiency in the workplace.

Transfer information easily

Numerous available tools enable you to generate digital invoices and quotations. Hence, your employees can instantly share relevant details without incurring printing and postage expenses.

Marketing and accounting teams can communicate information in realtime and make adjustments according to their clients' needs. Employees can easily search through old documents with a few clicks. They can arrange documents by date, clients, serial number, and nature of documents.

Enhance security

Even though cyber-attacks are frequent, digital documents have become more secure. Electronic records are easier to render through encryption.

You can control access to specific documents and manage security levels. Printed documents require a lot of space, and controlling access is not possible. Documents are also prone to fire and water damage. You can double up digital efforts with backups and cybersecurity.

Lower costs

When you transform documents digitally, you improve the process's efficiency and lower expenses.

Digital transformation offers you to store a large volume of paperwork, saving a lot of storage space. Moreover, digitalization will reduce the cost of ink, printers, paper, employee time, and space to store the documents.

The most important benefit of going digital with your paperwork is that you save employee time. They can perform additional tasks instead of storing, managing, and searching for documents.

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

Tech Tip: How's Your Video Call Etiquette?

Two years on, we're all **Video Call Champions** now. Bet that's a skill you never thought you'd master.

It's so convenient to hop on a video chat with a colleague to discuss a problem or clear up details on a project. You don't really think twice about it anymore, do you?

There's always room for improvement. So here are our suggested rules for good video call etiquette:

Create and share a meeting agenda

If you schedule a meeting with several others, let everyone know what the meeting is about and give them chance to prepare. If you use Teams, there's a text box at the bottom of the New Meeting invitation where you can add in details.

Make sure your background is suitable

Cameras on, everyone. Seeing people is the big benefit of video calls. While people may be intrigued about where you are, blurring your background or working in front of a plain wall will make sure the focus is on you and not your house.

Don't overshare

Ever been caught out when screen sharing? Maybe you've received a notification for a personal message, or even forgotten to close down a website before joining your meeting?

You can share only the application you want to show by clicking 'Share' and choosing the thumbnail shown in the 'Window' category.

Stand up

Want to keep your video calls focused and productive? Then get everyone to stand up for them. This might seem strange, but guess what? It works really well for in-person meetings you want to keep short and to the point.

Should You Monitor Your Remote Workers?

At the end of last year, Microsoft announced it would be adding increased employee surveillance to Microsoft Edge.

The changes mean admins can access compliance monitoring through the browser, such as seeing which files have been printed or copied to USB devices.

Machine learning is being used to increase this visibility of what's happening to sensitive files. But how will this impact employees? Will they feel that their privacy is being invaded? Will it cause trust issues? And do you think this is an appropriate level of monitoring when people have proved that remote work can be just as productive – if not more – than working from the office?

Our advice would be not to buy into this increased employee surveillance, unless you want to damage the delicate trust you've no doubt worked hard to build with your team.

There are other, more open ways to help your people get their work done.

For example, there are plenty of tools that help limit distractions like notifications or temporarily block apps and websites to allow better focus. Your employees can choose to activate these to aid their productivity when they need a boost.

You'll find some within your Microsoft 365 subscription – that means more tools at no extra cost.

If you want some suggestions personalized to your business, give us a call.

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

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.

Five Things You Should Never Do On A Work Computer

Whether you work remotely or in an office, the line between personal and work tasks can become blurred when working on your company computer. If you're in front of a computer for most of your time during work, then it's not unusual to get attached to your desktop PC.

Over time, this can lead to doing personal things on a work computer. At first, it might just be checking personal email while on a lunch break. But as the line continues to get crossed, it can end up with someone using their work computer just as much for personal reasons as work tasks.

In a survey of over 900 employees, it was found that only 30% said they never used their work PC for personal activities. The other 70% admitted to using their work computer for various personal reasons.

Some of the non-work-related things that people do on a work computer include:

- Reading and sending personal email
- Scanning news headlines
- Shopping online
- Online banking
- Checking social media
- Streaming music
- Streaming videos/movies

It's a bad idea to mix work and personal, no matter how much more convenient it is to use your work PC for a personal task during the day. You can end up getting reprimanded, causing a data breach at your company, or possibly losing your job. Here are several things you should never do on your work PC.

Save personal passwords in the browser

Many people manage their passwords by allowing their browser to save and then auto-fill them. This can be convenient, but it's not very secure should you lose access to that PC.

When the computer you use isn't yours, it can be taken away at any time for a number of reasons, such as an upgrade, repair, or during an unexpected termination.

If someone else accesses that device and you never signed out of the browser, that means they can leverage your passwords to access your cloud accounts.

Store personal data

It's easy to get in the habit of storing personal data on your work computer, especially if your home PC doesn't have a lot of storage space. But this is a bad habit and leaves you wide open to a couple of major problems:

Loss of your files: If you lose access to the PC for any reason, your files can be lost forever.

Your personal files being company-accessible: Many companies have backups of employee devices to protect against data loss. So, those beach photos stored on your work PC that you'd rather not have anyone else see could be accessible company-wide because they're captured in a backup process.

Visit sketchy websites

You should assume that any activity you are doing on a work device is being monitored and is accessible by your boss. Companies often have cybersecurity measures in place like DNS filtering that is designed to protect against phishing websites.

This same type of software can also send an alert should an employee be frequenting a sketchy website deemed dangerous to security (which many sketchy websites are).

You should never visit any website on your work computer that you wouldn't be comfortable visiting with your boss looking over your shoulder.

Allow friends or family to use it

When you work remotely and your work computer is a permanent fixture in your home, it can be tempting to allow a friend or family member to use it if asked. Often, work PCs are more powerful than a typical home computer and may even have company-supplied software that someone wouldn't purchase on their own.

But allowing anyone else to use your work computer could constitute a compliance breach of data protection regulations that your company needs to adhere to.

Just the fact that the personal data of your customers or other employees could be accessed by someone not authorized to do so can mean a stiff penalty.

Additionally, a child or friend not well-versed in cybersecurity could end up visiting a phishing site and infecting your work device, which in turn infects your company cloud storage, leaving you responsible for a breach.

At least 20% of companies have experienced a data breach during the pandemic due to a remote worker.

Turn off company-installed apps like backups and antivirus

If you're trying to get work done and a backup kicks in and slows your PC down to a crawl, it can be tempting to turn off the backup process. But this can leave the data on your computer unprotected and unrecoverable in the case of a hard drive crash or ransomware infection.

Company-installed apps are there for a reason and it's usually for cybersecurity and business continuity. These should not be turned off unless given express permission by your supervisor or company's IT team.