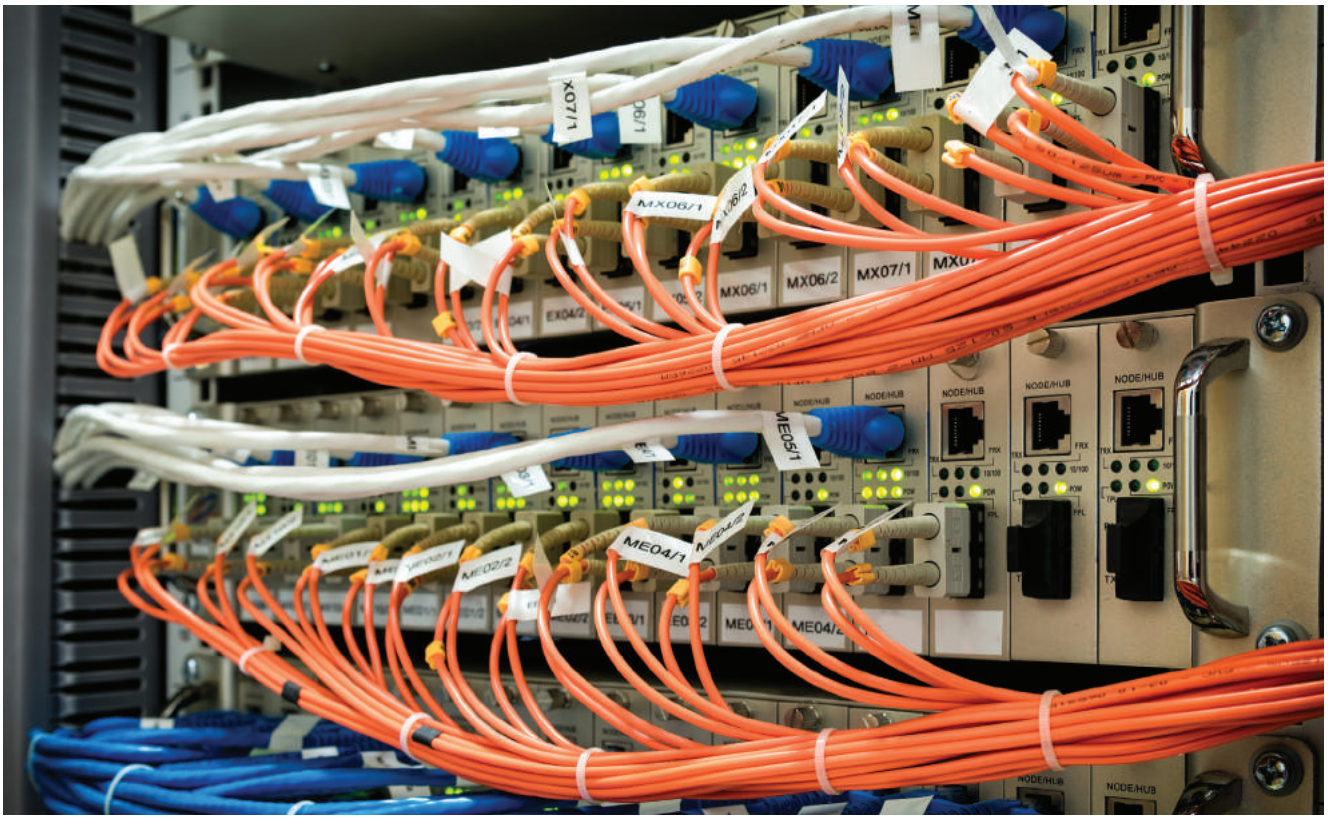

Importance of IT infrastructure in supporting digital transformation

As we move into software enabled ecosystems supporting fast moving digital transformation, the need for robust operational planning could not be more important, says Sachin Bhardwaj at eHosting DataFort.

IT infrastructure is no longer in the sole dominion of on premise installations and are gradually moving to the cloud. With rapidly changing market needs, there is a pressing requirement among businesses to be agile. This revolution has given rise to a never before threat that is all set to engulf most companies.

Digital security is no longer a passing thought. It is one of the most important challenges facing enterprises today. In fact, Gartner has predicted after due analysis that by 2020, 60% of ventures will experience major service failures because of the inability of the IT department to secure the scope of its digital infrastructure and understand the risks that are looming on the horizon.

Digital security is proving to be a tough nut for most IT departments to crack. And there are a few key reasons for this:

Digital threats are variable.

Every day, new advancements are being made in subversive malwares and request denial techniques. The attacks and their orchestrators are evolving faster than the security technologies that can combat them.

Digital security must keep threats at bay but should be flexible enough to support rapid scaling and growth.

Thus, protection strategies and their execution should accommodate the fast pace of digital businesses. This must respond to economic and demand fluctuations faster than their traditional counterparts are required to. However, the balance is a tough one to maintain.

Digital security paradigms must take into consideration technological diversity.

Bring Your Own Device is already immensely popular. Workers access data from their mobile devices, from the secure office portals and thanks to SaaS applications, even from their home. This complicates threat management.

The fluidity of access that is so critical to enhanced workplace productivity and telecommute poses challenges to infrastructure security. A wide range of devices have to be monitored and separate rules defined for access from multiple touch points.

Infrastructure and process of analysing digital threats

Experts believe that more than infallible security, enterprises need to focus on better response to possible threats. Thus, systems that are capable of learning and adapting are the most sought after solutions of the future.

A typical analysis of existing security covers the following steps:

1. Scoping of the infrastructure to understand its weaknesses and vulnerabilities. This dictates the upgrades and replacements needed to strengthen the foundation of the digital business.
2. Research and evaluation. Here the threat patterns for businesses in the industry are studied. Are malware installations more common or does DDoS seem to be the major challenge? If the business has suffered security breaches in the past, this data can also prove to be invaluable.
3. The final step pertains to structuring a security regime. This includes hardware and software security as well as background checks of employees. Use of strong commercially available ciphers, the purchase of security certificates and even implementation of a disaster recovery plan are common practices.

Infrastructure for an effective data backup plan

Whether technical failure or natural disaster, backup and disaster recovery solutions are an absolute necessity for organisations of all sizes. Putting time and effort into finding, implementing and maintaining a good backup and recovery solution should be your top priority.

According to a recent survey, data loss is increasing at a rate of 400% per year. An estimated $1.7 trillion is what businesses stand to squander if they do not invest in proper data backup. What's more? Even in this era of cutting edge technology, many organisations in the UAE claim that they do not have any disaster recovery measures in place. Three steps for an effective backup plan:

Sachin Bhardwaj, Director Marketing and Business Development, eHosting DataFort.

1. Designing the operational plan. Osterman research has shown that 75% of the data that employees need to operate productively on a day to day basis is hosted by email servers in the form of messages and attachments. Let us not forget the social media interactions with followers, clients and influencers that can prove to be invaluable research. The point is that everything around a business is a potential source of data and thus insights.

Backing up only the transaction records or the preferences of clients is just not enough anymore. Companies need to think outside the box. Consider all digital platforms that puts you in touch with the people who are vital to your business. How much of this data is irreplaceable? How much of this data is sensitive and should be backed up in an encrypted database? Without concrete answers to these questions, a fool-proof backup plan is not possible.

2. Planning for all contingencies. Is it enough to randomly back data up? No! Data backup costs money. And thus, businesses need to be very strategic with how they go about the process.

Redundancy is important. There has to be a back-up of the back-up of information that can't be recovered if it is lost.

Do not put all your eggs in one basket. Redundancy in terms of geographical location is also important. This kind of foresight mitigates the impact of disasters. Ensure that mission critical and sensitive data is backed up in multiple locations. And is easily accessible to the workforce.

Safety is paramount. Data loss is not the only problem that enterprises face. Data breach is another. Enforce security protocols like passwords and limited access permission for classified data and keep yourself and your backups well covered.

3. Testing your systems. Not testing a backup plan for operational errors and flaws is the worst mistake that a business can make. It is important to give the backup platform a test run as soon as it is implemented and do so regularly thereafter.

The key is planning, training, testing, and regular review of the plan. Do this and you will survive any trouble that you might encounter. ■

Consider all digital platforms that puts you in touch with the people who are vital to your business. How much of this data is irreplaceable?