



THOUGHT LEADER: HOW NEW TECHNOLOGY WILL IMPACT INTERNET CONNECTIVITY

October 23, 2017

The internet connectivity market is changing fast. Looking ahead to 2018, there will be some interesting trends that continue, but new technology will have the biggest impact on the internet connectivity landscape.

Demand for bandwidth will continue to grow

High bandwidth services are now required and expected for both consumer and business applications. Both segments are becoming more speed hungry; video has grown dramatically, and computing and storage is moving to the cloud.

The business benefits of cloud storage and computing having been proven. Forward looking businesses have already moved to the cloud and the late adapters are asking when, not if, they will move. Often the choice is being removed from business; most software vendors for applications like accounting software, CRM or phone systems are only offering new customers a software as a service (SaaS) model. However to get the benefits of cloud services, business need to ensure they have a fast, reliable internet service.

Young viewers now watch 2.5 times as much video via streaming than they watch on traditional television. Video now accounts for 74% of online traffic. Video is no longer just for consumers, businesses are using social and video platforms more and more. Giving employees good connectivity both in the office and on the move is essential for happy and effective employees.

These extra demands on business internet means customers are looking more at services like ethernet that come with service level agreements (SLAs) that have high availability guarantees. Suppliers like Verizon and AT&T are racing to get services available across the country with urban areas and business parks being the first to be lit.

High bandwidth Fiber services are also being rolled out with services like U-verse and FiOS pushing hard to light up new areas. We are seeing the prices drop massively on all these services, so it is worth reviewing regularly.

New Software Defined Networking technology means networks are getting smarter and cheaper to run

New technology is pushing the boundaries of what SME businesses can afford to deliver on their network. For those that do not live and work in an IT department, Software Defined Networks are the latest game changer in networking. They allow business to control how their network operates, what traffic it prioritises and how it is secured all from a single central access point. If that sounds a bit techy, then it is simpler to say that it gives all of the functionality of a huge companies MPLS network at a fraction of the price, all without needing a team of engineers to maintain it.

Going a little deeper, the 'software defined' bit moves all the intelligence and routing decisions away from the hardware and into software, which means it is much easier to control. Being software (rather than hardware) it also means you can program the service to run more efficiently. Consequently, if your connection to cloud servers need extra bandwidth, it will automatically throttle back someone watching YouTube on their lunch break.

The prices are competitive already (and a huge discount from legacy technology), so they will remain stable for the foreseeable future.. Product adoption in 2018 is going to be huge. The only thing holding companies back will be the requirement to upskill IT teams, and a for much larger companies, the requirement to coordinate effectively over a large network. Software Defined Networks have put the countdown timer on MPLS in the SME space.

The cloud will be the only choice...

... and I don't mean this from a 'it's great you just have to do it' sense, but from a 'you won't be able to buy anything else perspective. As above, the big software players have moved away from a licenced on premise software sale and have moved to cloud based SaaS model. There are many reasons for this; shareholders love predictable income, support costs drop massively as you can always push new code and don't need to support older versions, security is massively improved by gaps being able to be plugged fast and the customer experience tends to be better as well. The software is scalable, licences can be turned on or off as required and you normally know that you are getting the same deal as everyone else (no haggling!)

We will also see more hybrid cloud deployments. Hybrid cloud deployments use a combination of private cloud, public cloud and on-premise servers. The most critical applications normally sit in the private cloud (though sometimes onsite) and then the public cloud is used to burst for extra storage or power. This model can reduce costs vs. having a fully private cloud, while still getting a lot of the benefit.

However, as with all software, there are security concerns to be considered when using cloud technology. Arna van Goch, Founder and Owner of [Horizons21](#), says: "Cloud technology is growing at, quite frankly, an alarming rate. The reason for this can also be attributed to the countless hacking scandals that has rocked the political and economical worlds in the last year or so. With big cloud computing companies promising security measures and back-ups, not to mention 2 factor authentication (much to the dismay of office workers trying to keep their mobile phones separate from their work phones) and spot-checks of security, we are going to continue to see this trend develop. What will be interesting to see is the security measures that are supposedly in place."

The internet of things (IoT) will be a revolution (but also a security risk)

You may not have heard of the internet of things, but you will definitely have seen some of the products advertised. Smart meters for electricity, the home tech products like Google's Nest or the Amazon Dot (Alexa's home interface) are a few well known examples. These products are starting to cost much less, so adoption is going up at home and in businesses. However, as with anything on the internet, there are some serious security considerations. The default passwords on many of these devices are not being changed and this can give hackers access to many areas of people homes and businesses. As our world evolves and what was once mundane has now become incredible, we must remain mindful of these potential pitfalls.

Data security expert and former Google Executive, Charif Elansari, is well aware of the cyber-security risks and threats that businesses face in today's digital age. As CEO of [Dropsuite Limited](#), Charif understands the need for businesses, especially SMEs, to have access to a platform that allows them to easily backup, recover and protect their digital assets.

John Moor, Managing Director of [IoT Security Foundation](#), says: "IoT class devices and services are permeating every part of modern life, from the personal, domestic, vehicle and office to our critical national infrastructure. Along with the huge potential for innovation comes a real threat of connection, most significantly in regards to security and privacy.

"The world is moving so fast that standards and regulation not only struggle to keep up, but also risk stifling innovation if they are hurried. Yet the world needs answers, and needs to act now. There is good news however, as we already know how to improve security and privacy assurances to acceptable levels. This is through awareness, education and the adoption of best practices. To be successful, these need to be easy to understand and low, to no cost, to acquire. This is the role of the IoT Security Foundation."

[Ahmed Khalifa](#), Digital Marketer and online privacy and security enthusiast, adds: "With an expected 50 billion connected IOT devices by 2020 according to Cisco, the risk that comes with IOT mirrors those on other "traditional" devices like computers and tablets. Hackers can penetrate your IOT by accessing the public and private networks that are around the world and tools such as Shodan.io can enable the average tech users to do just that."

Multi site businesses are at increased risk. Steve Bennett of [OGL Computer](#) advised that "These sites are higher risk as data may be replicated between sites – centralising infrastructure and providing VDI or thin client access to systems is then prime to control access – this in turn enables the backup to be centrally managed."

But just like other internet-connected devices, the same best practices applies to IOT and these include protecting your WiFi network with strong passwords and firewall, have the admin to be responsible for user control, implement 2FA where possible.

Charif adds "Unfortunately, the human factor remains the weakest link when it comes to cyber-security vulnerabilities where it is estimated that more than 70% of cyber-security attacks occur due to human error."

Tracy Rock, Director of Marketing at [Invenio IT](#) emphasises this "Believe it or not, one of the greatest weaknesses in any business is its staff. While often unintentional, employees jeopardize cybersecurity in a variety of ways, such as: clicking on infected emails, not following proper protocol for saving data and installing unapproved software on work devices or bringing personal devices in to work, introducing potential vulnerabilities. Overall, we find employees just don't realize that their organization could be a target for cybercriminals and that they play a critical role in cybersecurity."

Data Security Precautions to take:

Backup, backup, backup. It seems like common sense, but there are an abundance of instances where even the most established businesses don't do the bare minimum.

Regularity of backups can vary wildly from business to business – Tracy Rock adds – "How often backups should be taken, depends on the business. We recommend anywhere from every 15 minutes to once a day, depending on importance of data. Backup systems need to updated as system updates are available as they can help detect and deter vulnerabilities."

Around 30% of Dropsuite's customers restore data on an annual basis, which speaks volumes on the importance of deploying backup systems to ensure business continuity.

<https://www.telcosolutions.net/blog/cloud/how-new-technology-will-impact-internet-connectivity/>