CIONET

DISCUSSION SUMMARY

BRING YOUR OWN ‘EVERYTHING’

This article was written by Roger Camrass, director of CIONET UK and a visiting professor of the University of Surrey, and is based on the conversations during a dinner on the revolution in end user computing, sponsored by Jamf in February 2020.

Over the next decade the workplace will change out of all recognition. The millennial and associated 'prosumer' workforce will expect to use a wide range of devices and applications to conduct their business as well as to run their family and social lives. The era of 'Bring Your own Everything' (BYoE) has finally arrived. In this context IT organisations will need to support a multiplicity of software platforms such as Windows, Android and iOS as well as devices (fixed and mobile).

BYoE is a part of a bigger picture

The plurality of devices, platforms and applications places growing emphasis on business risk, compliance and security for both commercial and public sector organisations. Delegates at the dinner argued that the new BYoE era is far reaching and includes the entire information 'supply chain':

- Authentication and permission for individuals (e.g. employees and contractors) to access appropriate data and related applications (e.g. multi-factor ID)
- Devices, both personal and corporate, that provide a gateway into corporate systems (from the office or home) as well as social sites
- The network connections that include fixed (e.g. desktop) and mobile/wireless (smart phone) links that operate over public or private facilities
- The applications and related data that are a primary corporate asset and need to be constantly monitored and protected

As discussed in recent dinners, employers have been slow to respond to the IT needs of employees, especially in the mobile domain. Little has changed over the last few years compared to the great progress made in supporting customers with mobile and online applications and connections. Productivity has suffered and many young people are moving jobs purely on the basis of poor end user support.
Do you treat your employees as customers for IT based applications?

Evolution of devices

Just ten years ago, the choice of corporate smart phones was divided equally between BlackBerry and iPhones. Today there are several players such as Samsung, Huawei, Apple, Nokia and Motorola as well as BlackBerry (now sold off to a Chinese manufacturer). Equally, the choice of tablets and laptops continues to grow as do the operating systems that support them (e.g. Android and Windows versus iOS). Most employees prefer to carry just one or two devices around with them – a smart phone and tablet. This places constraints on IT:

- Personal versus corporate: how can a single device be used for both purposes whilst protecting corporate data?
- Authentication – how does the 'system' recognise a specific individual and give them access rights to relevant corporate applications?
- Mobile versus fixed – how might access rights vary between a mobile (e.g. smart phone) and fixed (e.g. desktop) environment?

Many of these issues are especially relevant when people either join or leave an organisation. Delegates asked:

- How might onboarding contribute to employee satisfaction and loyalty?
- How can an organisation protect itself when a person leaves with possible removal of vital corporate data?

Converting data into value

The advent of 5G increases connectivity across the increasingly mobile workforce. It also enables far greater communications between sensors and other machine to machine devices. Employees are seeking to use their smart phones for communications of all sorts, from social media (e.g. Twitter and Facebook) through to video conferencing, collaboration (e.g. Slack) and traditional email. This includes domestic as well as corporate traffic. The boundaries here continue to blur as we enter a 24/7 work environment – anywhere, anytime, anyplace.

Whereas much of corporate traffic was confined to private, fixed network facilities ten years ago, the shift is now in favour of public facilities with the emergence of software defined networks (SD-WANs) that utilise public clouds such as AZURE and AWS. This implies higher security risks as highlighted by the very public debate over Huawei and the UK 5G network.

The answer is data encryption at source which will prevent any downstream breeches.

Data lakes and data warehouses

Most organisations hold their data in a multiplicity of fragmented corporate

applications, many of which are legacy. However, the recent move to 'data centric' architectures implies a coming together of different data types from these multiple sources. Organisations are adopting data lakes and data warehouses located in the public cloud to deliver such architectures. These changes require cleansing of current data and adoption of standard formats. In so doing, critical data resources become much more accessible both to employees and potential cyber criminals.

At the same time, organisations are employing many more data scientists and related tools to analyse these vast data resources. Data Lakes need to be partitioned to reflect the emerging team structures and associated applications – ranging from predictive analytics through to machine learning and AI. All of this takes thought and preparation during the migration to public cloud services. Aligning corporate data to relevant users will be a key challenge in the data centric world of the coming decade.

Organisations need to develop new 'data-centric' architectures for cloud.

Joining the end user revolution

Few organisations can now ignore the revolution taking place within end user computing. As one CIO recently stated, 'when I go to my office each day, I go back three generations in technology'. Such a situation cannot persist for much longer. Other CIO complain that to equip a large workforce with modern tools can take years and cost many millions, witness the roll out of Office 365 and associated Surface PCs. The resounding conclusions of the dinner were:

- Embrace the move to BYoE and encourage employees to adopt the devices of their choice- both fixed and mobile. This will improve productivity and loyalty
- Introduce financial incentives to enable individuals to purchase their own equipment – as an employment benefit
- Ensure security by encrypting all data that is available to employees, contractors and trading partners

Adopt 5G as the primary network to access corporate applications and provide web front-end interfaces.

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com