CIONET

DISCUSSION SUMMARY

RETHINKING WORKPLACE SECURITY THROUGH COVID-19

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 virtual meeting on 'Rethinking Workplace security' held in July 2020 and sponsored by Avanade.

Introduction from Richard Mardling, IDAM Director, Unilever

Imagine that you had just two days' notice to move over 100,000 staff from corporate offices to their homes in 200 countries around the world. This was the task given to Richard Mardling and his team in March of this year. The starting point prior to the pandemic was a network capacity able to handle 17,000 concurrent conversations. This had to increase to 68,000 connections over a single weekend. Equally, provision had to be made to handle up to 4,000 leavers and joiners each month.

The first response was to increase VPN capacity by adding six new nodes. However, it soon became apparent that hub-based traffic would rapidly reach a ceiling. Fortunately, Unilever had adopted public Cloud (AZURE and AWS) some three years ago to support Office 365, Workday and other SaaS services. This provided a suitable platform to by-pass VPNs and to open-up near unlimited connectivity across the globe.

The move away from VPNs to public cloud posed a major security challenge. Unilever needed to offer its staff convenience through 'single sign-on' to some 500 applications via public cloud. It chose a cloud-based product (by Zscaler) that enabled secure access. This delivered a 'zero-trust' environment that enabled staff to access applications and data from any location or device worldwide.

Post the transition to home working, Unilever's next challenge has been to facilitate a gradual return to the office, whilst offering a level playing field for those staff who prefer to stay at home. The prospect of hybrid work conditions (home and office) has created the need for different governance principles and associated security controls. What was most interesting about Richard's introduction was the emphasis on the 'employee' rather than the 'customer' experience – offering staff the most convenient way to access corporate applications and productivity tools using single sign-on ID, via public cloud connections. Microsoft 'Teams' has been particularly successful in connecting remote workers.

Richard mentioned that the move home coincided with 'year-end' reporting and closing of the accounts. This process was completed in record time despite the physical disruption to staff. Productivity does not appear to have been affected by a distributed work environment.

Success factors for a smooth transition to home working

The audience described several key success factors that enabled a smooth transition to home working. These included:

- Cloud rather than hub-based network connectivity (e.g. AZURE) – thus avoiding 'hairpin' routing via congested data centres
- Universal adoption of Microsoft Office 365 and associated productivity tools such as 'Teams' prior to the Pandemic
- A 'Bring your Own Device' (BYOD) policy that encouraged staff to use home terminals such as Tablets
- Citrix based virtual desktop that simplified end user support and took a big load off contact centres
- A phased transition to home working that could be implemented in a global environment – starting with Chinese staff

Critical security challenges

The wholesale move to home working has introduced several security and governance challenges such as email phishing attacks, oversight of expanded attack surfaces, possible third-party access to confidential client information (such was the case for a wealth management firm) and lack of end-to-end security controls. The need to move many thousands of workers in days called for speedy decisions that increased security and governance risks. This was accompanied by a noticeable increase in criminal activity, especially during the first few weeks of the pandemic.

Some in the audience described the need to adjust their risk assessment processes including revisions to the risk register. Of concern also was the lack of experience within the workforce relating to home working. This varied between sectors with global, tech and USA based companies more familiar with distributed working.
The transition to home working has tested leadership and corporate culture more than technical capabilities. Most IT departments were able to cope well with the transition.

Microsoft - a case example

Sarah Armstrong-Smith, chief security advisor to Microsoft, described how the Company had taken its own dramatic steps to cope with the Pandemic. Equipped with 160 data centres and a global network prior to the pandemic, Microsoft had sufficient capacity to handle the transition to home working both for its clients (for example, 25 million concurrent users of 'Teams') and its 40,000 staff. The data centres remained operational working largely under 'dark' conditions. Shortages of devices encouraged a BYOD approach.

Microsoft was quick to adopt a 'zero trust' environment to support its own staff, current and new clients. Security arrangements were paramount as Microsoft become the number two global target for cyber attacks (after the US Department of Defence). Leadership under Satya Nadella recognised the significance of COVID-19, describing the transition as a two-year transformation undertaken in two months. Much effort has been directed at employee wellness and safety with regular 50-minute meetings to brief staff and discuss issues.

Governance is at the heart of effective data management

One of the most interesting and contentious points of discussion was around the governance of corporate data. The big question for many organisations becomes 'who owns our data'. This ranged from the COO and CIO to central data science teams and CMOs. All delegates agreed that data is a business asset and needs oversight from a single corporate function.

IT has a vital but non-exclusive part to play here. IT tools such as data platforms can enable businesses to standardise and integrate data sources as well as providing the essential tools for its manipulation and consumption. However, it must be the businesses who have ultimate responsibility for ownership, especially in a data centric world. Again, much can be learned from digital natives who have organised themselves around their data. In the financial sector, regulation and compliance becomes especially relevant in deciding who controls the data. For example, Deutsche Bank has a central team reporting to the COO who are responsible for compliance.

Organisations need to build data governance into their enterprise architectures and assign appropriate functional responsibilities for operational and commercial data.

Lessons learnt and actions to be taken

Exchange of experiences during the virtual event illustrated the wide spectrum of preparedness and differences in speed of response to such an epic event. Overall, the lessons learnt included:

- Need for technical preparedness including full migration to public cloud (such as AZURE), early roll out of productivity tools such as 'Teams', and workable BYOD policies
- Regular communication at all levels of the organisation to ensure employee wellbeing and safety
- An ability to make rapid decisions and manage associated risks by adopting appropriate governance approaches
- Establishing security control processes to monitor who is on the network and who is on any individual device

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