SYMETRI
ADDNODE GROUP

THE EVOLUTION OF THE HYBRID WORKING MODEL

GROWING AND PROTECTING YOUR BUSINESS IN THE NEW WORLD

WHY READ THIS WHITEPAPER?

The Covid experience triggered a race for solutions that were new to many companies and could be rapidly implemented; technology ‘fixes’ that would get companies through the difficult times. It inspired fresh perspectives on the role and value of the cloud, serving a dispersed workforce regardless of distance or office presence.

This whitepaper presents a ‘check-list’ of those areas of your IT infrastructure which now merit revisiting, to help you make sure that the way your business works Is aligned to how the new business world has evolved.

INDEX

INTRODUCTION

MAKING THE ESSENTIAL ADJUSTMENTS

In July 2021, Symetri published a whitepaper looking at the new personality of work. The paper noted that: “The shift to home working is…about a fundamental restructuring of the processes and technologies that make it possible to work at a distance, across dispersed teams, without losing any of the productivity and quality outcomes that prevailed before”.

We were all adapting at that time. The process of business interactions changed. Companies’ views of how best to deploy technology had to be quickly reassessed to cope with the challenges of not just how the ‘new normal’ would affect their operations, but also how it could be addressed in a sustainable fashion for the long-term future.

This is where we are now—recognition that changes made were not just expedient, and possibly temporary, but are here to stay. Reassessment is again underway to consolidate new working structures.

NEW IMPERATIVES | CHANGING CULTURES

Following on from the pandemic, ‘Hybrid’ working practices for many, have stayed in place with varying weightings given to office attendance and working from home. Hybrid brings fluidity, agility, and a higher quality of work/life balance for employees[1]. Far from productivity and quality outcomes being undermined, they have been consolidated and improved. In some cases, huge savings have been identified from the closing of entire premises:

British Airways will let staff split their working lives between the head office and home in another example of big firms offering flexible employment. The airline is also exploring the sale of its huge Waterside HQ near Heathrow Airport, where 2,000 people worked before the coronavirus lockdown."[2]

Considerations also include the need to ensure that company culture does not dissipate. Employees feel the need to meet in person and not just in front of screens, so that the true quality of personal interaction is not lost, and that people feel part of something—motivated, supported and supportive.

The infrastructure that drives these outcomes also requires consolidation and, in some cases, improvement. Along the way to the new nature of work scenario, pressing focus areas have become evident, assuming a greater importance than they may have had before. These include a far greater need than ever for:

- More focus on security: an increase in devices in more places create greater security issues.
- Seamless online communications: easier online sharing of documents and files is essential.
- More reliable remote collaboration: the digital environment must not represent a reduction on productivity compared to physical interaction.
- Contingencies for business continuity: a ‘catastrophe’ should never be more than just a minor inconvenience.

THE DRIVERS FOR CHANGE

KEY QUESTIONS TO BE ANSWERED

‘Business as usual’ has largely been resumed for most organisations. The widescale move to the practices of the ‘hybrid office’—part home/part office—has led to almost universal adoption of online communication and collaboration platforms. Symetri’s previous whitepaper on this topic evaluated two scenarios for contending with the changing nature (and the new diversity of locations) of work and IT infrastructures, for them to roll on just as productively and as efficiently as they had before any change had been thought necessary:

- The office at the core, with the ‘home’ at the edge.
- Home as the focus, with an office connection.

The second scenario is becoming more firmly entrenched, globally. More and more companies are moving to permanent flexible work models.

ADOBE: "WHERE WE LANDED IS THIS: THE FUTURE OF WORK AT ADOBE WILL BE HYBRID.
1. Being digital-first will be critical;
2. Flexibility will be the default;
3. We’ll gather for the moments that matter;
4. Remote work will expand."[3]

This is not to say that the physical office shows any likelihood of completely disappearing since, for many, the very real need to meet and collaborate in person remains of key importance. The sharing and collaboration of data online is one thing (it can be done, although internet speeds may play a part in how quickly it will be done), but being together to discuss and make changes, generate ideas in the moment, and reach results right then and there is more motivational and involving.

There is a balance to be struck; a workable mid-path that connects the two ways of working. The core considerations in mapping out this path for the benefit of your business focus both on the technology you need to be confident in, and the preferences of the people you depend on.

CORE CONSIDERATIONS:

THE VIRTUAL PRIVATE NETWORK (VPN)	CYBER SECURITY ISSUES	BUSINESS CONTINUITY	CLOUD OR ON-PREMISE
Has your VPN retained relevance/effectiveness? Do you experience problems with slow connections?	With a dispersed workforce are you absolutely sure that your data is safe? Have you taken the expanded edge of your IT estate into account?	Do you run regular back-ups and/or ensure redundancy (duplication in case main systems fail)? If you do, is it all manual or automated?	Have you considered a move to the cloud to bring more agility to the hybrid working style? Perhaps you're already using the cloud and are thinking of exiting from it due to fluctuations in costs?

THE ROLE OF THE VIRTUAL PRIVATE NETWORK (VPN)

Dependency on the VPN is waning in the Architecture, Engineering and Construction (AEC) and Manufacturing sectors primarily due to the disparity between the file sizes that characterise much of the workflows (large files in particular) and the connection speed at which a VPN can transmit the files. It can be almost untenably slow. This creates frustration, at best, and can noticeably impact productivity, at worst.

Any technology consideration must also pay due heed to the impact it has on users. Dynamic and creative professionals do not want to be hampered by the tools of their craft; they want these tools to extend their capabilities, to align to the speed of thought and to accelerate the speed of progress.

Your users will nearly always have a high degree of familiarity with the possibilities and potential that technology can unleash. This empowerment is often a catalyst in their own career paths. If they feel blocked by outmoded tech, their motivation drops and they may even look at other employers where ‘state-of-the-art’ is a given.

Our last white paper stated that a VPN is effectively an interim approach to remote connection, particularly in the AEC & Manufacturing sectors with the file-size issue. When home working was in its infancy, the odd wait here and there for a file to come through was not onerous; a chance to attend to other small matters while the file downloaded or go off and make a cup of tea. However, home working has now progressed from that point and this can no longer be the case on a regular basis.

Working from home should not mean working at a disadvantage — less technologically supported than working in the office.

Reviewing models across dispersed teams across a VPN is a process somewhat at odds with the capabilities that the digital world can really offer.

There is increasing recognition of the flexibility afforded by Software as a Service (SaaS). Applications in the SaaS model are delivered through the cloud and accessed by users through the internet. As this trend grows, companies are becoming increasingly aware of other services they can access and other advantages they can enjoy; from enhanced cyber security to more efficient collaboration, automated back-up and storage, reliable business continuity and far more rapid transmission of files.

"By 2023, 60 percent of enterprises will phase out most of their remote access virtual private networks (VPNs)." With pandemic concerns kicking in since then, that estimate might have increased. [4]

FOCUS ON SECURITY

CYBER SECURITY

The security of data and systems has always been a business priority. When they were the identifiable central core of business activities and operations it was important to ring-fence them (or at least firewall them) so that unwelcome/unauthorised outsiders could not get in.

With the dispersal of workforces, the cyber security consideration has become more complex. The core is no longer central, the perimeter has expanded, hacker entry points have proliferated, devices have multiplied, and demarcation lines between where work begins and ends have all but disappeared.

You need to have a clear view of how your IT estate now comprises nooks and crannies that have appeared as a result of best intentions (to keep the business and communications flowing through times that were extremely difficult and often required ingenuity) but that often appeared through tactical thinking. They may not necessarily have been notified to administrators. They just merged in. The danger is, that as they did, they sat outside the core and beyond any protection thereby afforded.

Be cyber-aware; if you're connected, you're a target. In the digital world, all data is sensitive in the wrong hands, and there are many wrong hands everywhere trying to access it. From financial information to account access, from customer records to Intellectual Property, from project plans to personnel files; it all needs to be protected.

Of equal importance to the need for protection, is the need to be seen to have robust and proven cyber security strategies in place. Clients expect such strategies by default. For projects coming from government departments, they are mandatory.

The dispersal of workforces, and the rapid shift to home working, exposed weaknesses in centralised cyber security. More entry points became available to even the most unsophisticated of hackers. As for the determined, organised, and well-resourced global community of advanced cybercriminals, opportunities blossomed.

1 in 6 Construction firms hit by ransomware[5] attacks[6].

CYBER ESSENTIALS

For AEC and Manufacturing companies, a secure IT infrastructure is a pre-requisite for many government contracts or tenders, particularly those requiring Building Information Modelling (BIM) procedures and practices.

Being able to prove robust security strategies and policies is where external validation comes in—it shows that your security measures have been audited by an independent third-party and are deemed fit-for-purpose. It reassures customers both of the quality of your approach and that any data passing between you and them will be as safe as it can be.

Spring-clean your security

External validation of your security measures is most commonly provided by Cyber Essentials[7], a certification scheme offered by the National Cyber Security Centre (NCSC), a UK Government organisation.

As important as the certification itself is the process you need to follow to obtain it. There was a time when the questionnaire you needed to complete, to gain certification, numbered around 50 questions. Today it is closer to 100. It is a rigorous process that forms the basis of a best practice audit of your security practices, and will encourage you to look into those areas you may not yet have considered or were simply overlooked during the changes happening over the last few years.

What is Cyber Essentials?

“Cyber Essentials is an effective, Government-backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber-attacks”.
National Cyber Security Centre

Cyber Essentials: Requirements for IT Infrastructure v3.1

Download the updated Cyber Essentials Guide

Extensive changes have been made to the Cyber Essentials process, many arising from the lessons learned when the world made its shift to home working. A specific section on home working states that “… all corporate or Bring Your Own Devices (BYOD) (home working devices) used for applicant business purposes within the home location are in scope for Cyber Essentials”.

The diagram, (from the above document) shows the boundary of the scope. Any device or service inside the boundary needs to be included when applying for Cyber Essentials certification.

In general terms, requirements for certification cover five technical control themes:

- Firewalls: preventing unauthorised access to or from your private network.
- Secure configuration: eliminating vulnerabilities in your network.
- User access control: limiting privileges to allow for a more secure and auditable process.
- Malware protection: protecting against viruses, worms, spyware, ransomware, and other external threats.
- Device security management: ensuring your devices are running supported operating systems and are kept up to date to patch any known exploits; ensuring also that software is supported, up-to-date and compliant to address any weaknesses found.

Symetri are Cyber Essentials certified. We can guide you in the right direction to become more secure and gain your certification. As important as the certification itself, is the process you need to follow to obtain it. We are happy to work with your current IT incumbents or provide our own IT support services to help your business go through the process.

BUSINESS CONTINUITY/DISASTER RECOVERY

It is essential that operational disruptions are kept to a minimum no matter what their cause. A power outage, for example, or a natural disaster such as a flood, can lead to loss of data if it has not been backed-up.

More than the loss of data, without adequate back-up if the moment comes, you stand to lose progress, waste time, lose money, and raise questions amongst clients about the reliability of your IT infrastructure and support.

Robust back-up is about far more than simply sending files to an external USB drive. It is also about more than relying on any included back-up features that come with the software you use. You will find that whilst many commonly used software solutions offer a back-up feature, the recovery period is not infinite.

Best practice is to make sure your files are continuously backed up, with data replicated off-site, ensuring business continuity and rapid disaster recovery. Best failsafe philosophy is to ensure that everything is backed up forever[8].

CLOUD OR ON-PREMISE?

How robust are your software solutions for enabling collaboration? Do they lack features you now believe you need? Is technology alone sufficient for the interactions important to your business?

What if your infrastructure were not on your premises, in the same way that your teams are now not as often on your premises as they used to be? As businesses more closely evaluate the 'as a Service' model they are exploring options where the suffix applies to more than just software. Infrastructure, Platforms, Disaster Recovery, Desktops and Devices, Virtualisation and many other aspects of IT are now available as a Service.

Such 'services' are based in the cloud. Any organisation can access the cloud from an internet browser. We all do this every day; this is where web-based email sits. If you are simply using the internet to gain access to anything 'as a Service', while retaining on-premise infrastructure and depending on a VPN, you will likely remain susceptible to the potentially disruptive effects of downtime (through power outages or natural disasters) and the sluggishness of VPN transmission speeds.

Associated maintenance costs of an on-premise infrastructure will still affect your finances. If anything goes wrong you will still be liable. With a dispersed workforce you will still be using collaboration tools to which there are more effective alternatives available with a cloud model.

Full adoption of cloud services is often accompanied by shifting the infrastructure out of your business. It can all be hosted in a datacentre. The immediate benefit is no more on-premise worries about downtime; no power cuts, no server access issues, no maintenance costs. There was a time when organisations were concerned that their data may not be housed in the UK, but leading cloud providers (such as AWS, and Microsoft Azure) now have datacentres in the UK, as well as offering robust cyber security.

However, the cloud/datacentre option is not for everybody. The size and volume of your business should be taken into account. Your investment in and commitment to legacy IT infrastructure should be taken into account. One of the operational benefits of cloud computing is its ability to scale as your business grows. Scalability is instant, with no need to worry about new hardware investment. Divesting your business of computing costs if you need to scale down is equally instant, since you will not find yourself burdened with hardware that you are underusing, and for which the ROI is diminishing. The caveat to be aware of here is that although your computing/technology costs will shift from CapEx to OpEx they may become less forecastable, and should therefore be closely monitored.

CONCLUSION AND RECOMMENDATIONS

It is now broadly accepted that hybrid working is here to stay. It is no longer a trend, or a reaction to imposed constraints; it is the future of work. You are likely to have already laid the foundations for this future, over the last few years. Now is the time to put those foundations to a stress-test and ask if you have embraced hybrid as an opportunity and not resisted it as an imposition.

In all the areas discussed in this whitepaper—the state of play with your VPN, the depth and strength of your cyber security, cloud and datacentre options and, most importantly, where to begin—Symetri can help you make the right decision for a better future.

ABOUT SYMETRI

Symetri creates and provides technology solutions and services for design, engineering, construction and manufacturing businesses. We empower people to work smarter for a better future by ensuring they have access to the expertise and technology they need to improve their performance and sustainability. We build long-term relationships with our customers and save their business resources by making technology easier to implement and use.

Our services include the provision of software, consulting, training and support, and we offer a comprehensive range of IT and Document Management solutions.

For further information, visit: www.symetri.co.uk

DOCUMENT REFERENCES

[1] Office for National Statistics | Is hybrid working here to stay?

"More than three-quarters (78%) of those who worked from home in some capacity said that being able to work from home gave them an improved work life balance in February 2022. Half reported it was quicker to complete work (52%) and that they had fewer distractions (53%). Almost half also reported improved well-being (47%)".

[2] Companies announcing a hybrid work model: Build Remote.

[3] The future of work at Adobe: Adobe Blog.

[4] Death Knell for the VPN?: Virtualization Article.

[5] Ransomware: "A type of malware that makes data or systems unusable until the victim makes a payment". (National Cyber Security Centre).

[6] In year to July 2021; reported by CyberTalk.org

[7] NB: You may also consider ISO 27001, but this is not a requirement for public sector projects, whereas Cyber Essentials is.

[8] NB: Not all data can be retained indefinitely. See our advice on GDPR.

LEARN MORE AT:
WWW:SYMETRI:CO.UK

SYMETRI
ADDNODE GROUP