Checklist for SMEs – new remote working tools

MCA

A POSITIVE FORCE FOR THE ECONOMY

1 BE CLEAR

Although COVID 19 has many immediate challenges and obstacles, there are also opportunities to develop the long-term strategic advantage of a business with new remote working tools. Consider what do you really need new technology for, for how long and for how many people? There are a number of areas to consider including:

- Document sharing and storage.
- Team Calls (voice or video) and messaging.
- Will meetings need to be recorded or not?
- Task or project management?
- Are edit locks on documents required and how will documents be approved?
- Will you be sharing company confidential or client sensitive materials?
- Do you need other technology such as headsets and webcams etc. and are there mobile applications on smart phones and tablets?
- Does the technology make sense from the user's perspective and how will you use it to stay in touch with your existing clients and customers?
- Does the technology align with any broader transformation and strategic plans and will this way of working become the 'new normal'?

2 IS IT SECURE?

Safeguarding your company reputation, your intellectual property, and the trust of your customers are top priorities for most companies. It is important therefore that security plays an important role in the choice of collaboration tools.
The following steps will help you to safeguard your information:

- Make sure staff have a good awareness of cyber security and consider regular online training.
- Design some simple do's and don'ts for your users – examples here would include:
  - Basic but still often over-looked elements such as robust password protection.
  - What type of data you are prepared to share externally and internally during this period and document this for the benefit of all users.
  - Can you limit who can join a meeting? Consider use of permissions and codes to access some or all internal and external team calls depending on the confidentiality or sensitivity of the discussion.
  - Management of rights of access to applications, systems and data must be sustained through remote access methods.
  - Consider how any third-party inclusion will be managed within a remote working environment e.g. access to project data and inclusion in meetings.

CONTINUES ▼

- Look out for providers who offer features like:
  - Data encryption (preferably in transit and in rest also). This may only be a requirement if there is sensitivity of content.
  - Two factor authentication.
  - Analytics or audit logs.
  - Providers who have achieved security standards such as ISO 27001, ISO 27018 and membership of regional security alliances.
  - Consider security accreditation of staff and also accreditation of technology through one of the many cyber accreditation schemes.
  - Remember, users working remotely from home tend to be more prone to targeted cyberattacks like Phishing.

- Use the administrative controls and user permissions that exist in many of the tools to make it harder for unauthorised access to your systems. In here you can control things like:
  - The ability to create, add, delete, restore and view.
  - Whether the community is private or public.
  - Setting up codes or passwords to join groups or calls.

- Monitor behaviour over time – some tools provide basic analytics to show usage and sharing, monitor on a semi-regular basis to identify.

- BYOD (Bring your own device) will add significant security risks to any remote access and should be mitigated where possible through other means (e.g. virtual, desktop, portal).

3 IMPLEMENTATION AND SUPPORT FOR YOU IF SOMETHING GOES WRONG

In some cases, the vendor will be able to offer after sales care for users. Is there a single number email address and/or support portal that users can go to for user support services? Failing that you should look for a tool which has a large, active and well-established online user forum which effectively acts as a Global Q&A function.

CONSIDER:

- Can you pilot or demo the technology with a small group?
- How will you roll out the new technology?
- What will you do if you have non adopters?
- Are there any policy, process or role changes that need to be incorporated?

4 SUPPLIER AND COMMERCIAL QUESTIONS

- What is the real long term need for access through remote working, and is this going to be part of an operating model that will require investment going forward?
- If a remote access service is ‘free to use’, consider what the commercial model of the supplying organisation will be, and the terms and conditions of use, including the potential for sharing of data and on app advertising.
- What are the licencing models that are available in the short, medium and long term, and can they sustain a need to both grow, and reduce usage?
- Can services be purchased as a commodity, and therefore be switched on and off as required by the organisation?
- Are the suppliers being considered the type of suppliers that will provide a long term, sustainable service, and work as a service partner with the appropriate service guarantees?

5 CLOUD SERVICES – AREAS TO CONSIDER

- Are there options for adopting software as a service to remove the need to manage core business applications, and are those services provided on a fully remote access service?
- Are there options for the application as a service, providing basic desktop and other general desktop tools (e.g. project management), and are these tools provided as a fully manged service?
- Are there options to use cloud services for user authentication and single sign-on, to allow access to multiple/all services provided for remote working?
- Are there options that allow the integration across different remote working services so that all aspects of working are joined up, and so that data can be appropriately shared across different services, systems and applications?

6 GLOSSARY

BYOD

The practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes.

DATA ENCRYPTION

Data encryption translates data into another form, so that only people with access to a secret key or password can read it. You should be looking for your vendor to be referencing that they have built their software in line with Advanced Encryption Standards (AES) which has been adopted as a global standard. A simple web search will tell you this – Does <insert vendor> have AES encryption?

TWO FACTOR AUTHENTICATION

An additional layer of security requiring the user to confirm their identity in two ways. Typically, they consist of:

- A piece of information like a password.
- Something which that user has (their work PC or mobile device).
- A biometric signature like a fingerprint or Face ID.

SECURITY STANDARDS

Show a level of maturity and diligence in achieving a set of industry standards designed with the intent of improving security for all.

- ISO 27001 – Information Security Management System.
- ISO 27018 – Protection of Personally Identifiable Information.

7 WHO ARE THE MCA?

The Management Consultancies Association (MCA) is the voice of UK consulting sector. The MCA is the representative body for the UK consulting sector and has been at the heart of the industry for over 60 years. We have a wide membership base and our members include PwC, Deloitte, EY, KPMG and IBM as well many other medium size firms and small specialist consultancies. Management consulting firms provide a broad range of services, from help in defining strategies to implementing large-scale IT and change programmes, and from coaching individuals and teams to providing expert advice in specialised fields.

The UK consulting industry is extremely competitive and includes a wide diversity of types of firm and specialisms, providing clients with the means to access precisely the support that they need. Requirements vary enormously – from highest level strategy and policy development to the achievement of specific financial and organisational goals. Common to them is the need to deliver tangible value for the client organisation.

Through our Consulting Excellence principles, which our members sign up to – members commit themselves to high standards in terms of ethical behaviour, clients service and value and professional development. They provide excellent consulting services which deliver the outcomes clients seek and need and they always strive to improve the value we can deliver to clients.

MCA
A POSITIVE FORCE
FOR THE ECONOMY

Management Consultancies Association

5th Floor,
36-38 Cornhill,
London
EC3V 3NG

T: 020 7645 7950
www.mca.org.uk
@TheMCA_UK

The MCA directory also has a full list of Consultancies and the sectors they specialise in.
PLEASE CLICK HERE

Thank you to **Integration Consulting**, **Mason Advisory** and **Sysdoc** for their contribution.

CONSULTING
EXCELLENCE