COVID-19: HOMEWORKING PRIVACY & SECURITY – THE NEW 'NORM'

INTRODUCTION

It is inarguable that the COVID-19 pandemic had had considerable impacts on the way we live our lives and the way we conduct our business. Whilst we search for the 'new Norm' what does not change are the legal obligations and moral responsibilities upon organisations to take all practicable and reasonable measures to maintain the security and integrity of personal data irrespective of its form.

Businesses responded to the operational challenges the pandemic introduced with great agility and facilitated many personnel to work from home. Homeworking (teleworking), something that was perhaps a luxury for a relatively small percentage of the workforce, has become the 'new Norm' for a much larger proportion of the working population.

As we settle into more routine business activities there is an opportunity to take stock of the situation and to consider things that may have been overlooked or measures and controls that might need to be reinforced.

This paper intends to promote various thoughts and pose questions for your consideration, whilst extending and complimenting two previous articles; details and links to which are at the end of this paper.

HOMEWORKING – PRIVACY CONSIDERATIONS

Many people now successfully work remotely from their kitchen, living room, study, shed or even their bedroom; often with children, spouses, partners and various pets sharing the same space.

Under normal circumstances, the family would not be granted physical access to your working environment or get anywhere near to your business data, yet you can now see and hear them during various online conferences and telephone calls. (I have lost count how many people have had drinks brought to them during online meetings / conferences).

Consequently, business information and personal data relating to customers or employees is dispersed to homes around the country, or even further! Such information rarely left the sanctuary of the office with its various physical and logical security controls.

Whilst many standard logical controls and measures to access the device and business data will likely exist, other points for consideration include but are not limited to:

- Do other family members have a conflict of interest, work for a competitor in the supply chain, or could there be an unauthorised exposure and data breach if family members had access to the information, which includes viewing content on the screen?
- Do staff, working at home, lock their screen when they go to the toilet or when they make a cup of tea?
- Do family members, as such unauthorised persons, have access to the work device for 'personal use'?
- Are staff working from home using their own devices and, if so, how do you assure the security and integrity of that device, the various software and applications running on it alongside business data?
- During online conferences, there is a tendency to screen share to facilitate information exchanges but do people consider other open files on their desktops, the email notifications and alerts that pop-up in the bottom corner of their screen?
- Have you evaluated the online / conference facility being used? Products such as 'Zoom', which may be acceptable for family gatherings and interactions, are not recommended for sensitive business information. Where your business is using such platforms have you defined any business rules (policy) regarding security options including but not limited to: waiting rooms and access password requirements? Have you looked at the information people are displaying in the background whilst online?
- It is likely that few people will print information at home, but there is a possibility – what happens to it, how is it safeguarded, does it get thrown out with the household waste?
- Have you undertaken and documented any form of risk assessment to capture the 'new Norm' of remote business operations, some businesses will likely remain in such working conditions for a reasonable time yet. There will be no flick of a switch and a return to previous working practices.

SECURITY TRAINING

We have seen an exponential rise in malicious emails looking to exploit weaknesses in our processes and controls. These are often targeted at our workforce, they aim to attack our end-points where the users are more vulnerable and susceptible to making mistakes.

We need to consider reinforcing and strengthening our security and data protection training. Not just regurgitating the old messages, but to further raise awareness and encourage the appropriate behaviours that will safeguard business operations. The last thing organisations need at this time is to lose operational effectiveness through a malware or ransomware attack.

DATA MAPPING

Acknowledging that these are not normal times and you have consequently remodelled business operations, have you considered updating data flow maps - the ones created as part of your GDPR preparations to satisfy Article 30 Records of Processing activities?

Information security standards such as ISO27001 require changes to business processes and systems to be risk assessed such that the organisation can reduce the risks and potential impacts to safeguard information assets.

The GDPR (Article 25) and the UK Data Protection Act mandate the principle of Security by Design and Default and the production of supporting materials that record the status of information processing activities. Again, given that the current situation is likely to be sustained for some time, how far have you progressed in evidencing and documenting what you have achieved?

In the event that you suffer a data breach or other unsavoury adverse event, do you have the right information to be able to demonstrate to the Information Commissioners' Office (ICO) that you took all reasonable precautions to safeguard the personal data?

A number of businesses have already stated that not all operations will return to where they were before the pandemic. They have realised they can work as efficiently and effectively from diverse locations, meetings can take place and decisions can be made without everyone being physically in the same room. Such diversity may become the 'new Norm' for some organisations. Now is the time to document and evidence the new data flows.

You may also need to refresh the Privacy Notices that inform customers and business partners how and where you process their personal data.

DATA PRIVACY IMPACT ASSESSMENTS

A further consequence of the changing landscape is the need to revisit or conduct data privacy impact assessments (DPIA) to reflect the changing ways of working.

DPIAs are a living document that must be maintained to reflect operational changes and processing activities. They are a powerful tool through which to identify areas of risk and exposure, to consider whether the appropriate controls and procedures are in place for the long-haul.

DPIAs are another useful and potentially powerful tool in the event of a data breach or adverse event to be able to demonstrate the thought processes and considerations that were made at the time.

DATA PROCESSORS / SUPPLY CHAIN

COVID-19 has directly impacted data processors and the supply chain who, of course, are also home working.

Hopefully there have been constructive discussions between the parties to confirm and agree the strategies and processes implemented. How are they being validated, monitored and in some instances even audited to verify their effectiveness?

Consideration should also be given to the countries and territories where suppliers and developers are operating from in support of your business operations. Where are they in their COVID-19 journey in comparison to us?

Global operations and dispersed supply chains and processing activities can be challenging at the best of times. Now there are new and very different factors to consider when it comes to outsourced development and operational support activities. These should be documented and properly risk assessed.

EXTERNAL AUDITS & CERTIFICATIONS

As the 'new Norm' of lockdown and dispersed operations continues, there will be an increased need to undertake audits for ISO27001 and PCI DSS compliance (to name only two) in order to attain or retain certifications.

ISO27001 requires the "understanding of the needs and expectations of interested parties" – how can you evidence that you have achieved that to preserve information security and data privacy requirements?

Organisations need to have reflected the changing circumstances and 'current operations' in their policies and processes in order to satisfy the auditor they have met the criteria for the certification. IRM has been conducting various remote audit activities in recent weeks and there's no doubt there will be many more in the months ahead. We have been looking for suitable evidence that organisations have considered the wider factors and implications that affect its ability to achieve the intended security and privacy outcomes of their certification programs.

SUBJECT ACCESS REQUESTS

Organisations are not given any reprieve during the pandemic to unnecessarily delay responses to subject access requests, unless it is possible to articulate why it is not possible to provide an appropriate and timely response due to the current crisis.

Organisations should be able to (legally) defend their actions if faced by a challenge from the requestor and the Regulator should the case be passed on to them.

DATA BREACH REPORTING

Organisations are still required to report data breaches, within 72 hours of becoming aware of the breach, in accordance with legal and regulatory obligations. Whilst the ICO has stated they will take "a more flexible regulatory approach"[1] this does not mean they will not take action even if that is taken some months later.

During an investigation and any subsequent enforcement actions, consideration will be given to the challenges and impacts of pandemic that were faced by the organisation. This may translate into a reduction in the level of monetary penalties linked to economic impacts of the pandemic. However this should not be taken as a lowering of standards.

MANAGEMENT OVERSIGHT & REPORTING

Management oversight and reporting is something that should be part of business as usual activities, even in these challenging times.

Adopting policies, procedures and supporting documentation that reflect today's operations are important; some organisations have created materials specifically for use at this time with the hope and intention of repealing them when the situation returns to normal or further revising them the reflect the 'new Norm'.

[1] ICO statement 15 April 2020 - https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/how-we-will-regulate-during-coronavirus/

EMPLOYEE COMMUNICATIONS & MANAGEMENT

Amongst the almost instant changes forced upon organisations and the restrictions imposed on individuals, management has had to become more widely involved in employee communications. Staff at all levels have been caught up in the emotion and anxiety of the situation they have been thrust into, they are looking for direction as to what they should do, at a time they are worried about their personal wellbeing as well as what this all means for their future employment.

Some employees are finding working from home extremely difficult, not least because the boundaries of work and home life have become entwined. Finding the 'new Norm' gaining a 'work / life balance', struggling with almost perpetual conference calls is physically and emotionally draining – there is nowhere to hide (unless they turn the camera off).

The days of team meetings in one physical location, at least for the foreseeable future, are probably consigned to distant memory. Team meetings and collaborations will need to take on a new and perhaps innovative way. Organisations that find the right dynamic will become stronger, those that do not will suffer the consequences.

Some people will not want to, or perhaps will not be able to continue working this way but will seemingly remain loyal to your organisation only because they fear the lack of alternatives; how will you support them in the weeks, months if not years ahead!

PLAN FOR THE FUTURE

Organisations have started to consider what their future operational model will look like and for some, a phased return of staff. This will likely need to consider continued social distancing within the office which necessitates changing office layouts, staggered routines to avoid overcrowding during the journey to / from the office.

A proportion of the workforce may continue to work remotely indefinitely thereby creating a 'new', 'new Norm'. This in turn will need to be reflected in your policies and processing activities for compliance certifications etc.

Business decisions regarding transformational change previously took management teams months if not years to ponder over. COVID-19 has forced organisations to take quick and decisive actions in days or even hours.

We are perhaps very fortunate that the pandemic did not happen four or five years ago; I for one have been surprised by the resilience of the core internet connectivity which has withstood a massively changing dynamic and demand placed upon it in such small timeframe.

ENVIRONMENTAL ISSUES

Have you had the opportunity to look at the night sky, and notice how clear it has been, how easy it is to identify constellations and to see the International Space Station? The air is cleaner and less full of pollutants. Perhaps COVD-19 has achieved more for the environment than any climate activist could ever have hoped for. No I am not a climate activist, but I do enjoy the outside life and am extremely fortunate to be able to run in the countryside – honestly, it has never been so good.

As you plan your future business operations carefully consider what the 'new Norm' should be – you will never have another opportunity to affect it like you have now – please do not waste it.

SUMMARY

Businesses have overcome significant challenges and changes to their working practices and environments. Individuals are more comfortable and conversant with remote working, using video conference applications and collaborating with their colleagues online.

We are at a point in time where this has become the 'new Norm' and there is a need to take stock of the situation and assess where business operations and data processing activities have changed to document them in case there are challenges or requirements to answer for at a later date.

This paper cannot address all the points for consideration, but hopefully it has provided some points for thought, guidance and direction.

COVID-19 has inadvertently accelerated business transformational change in ways that were unimaginable only a few weeks ago. As a consequence, organisations need to embrace and further develop the 'new Norm' very many will not go back to the same ways of working that they had only two months ago!

THE AUTHOR:

Paul Sexby – Head of Strategic Practice (paul@irmsecurity.com)

If there are questions arising, or if further assistance or advice would be beneficial, please contact IRM (hello@irmsecurity.com) or Paul directly.

Paul has also written other papers in this series:

- **"Practical Pandemic Planning (P3)"** providing organisation some practical advice and guidance consider in their preparations: https://www.irmsecurity.com/resources/practical-pandemic-planning-p3-coronavirus-COVID-19/
- **"COVID-19 –Data Protection & Cyber Security"** – addresses some of the considerations pertaining to data protection, remote working and human factors: https://www.irmsecurity.com/resources/covid-19-data-protection-cybersecurity/