COVID-19 – GOVERNANCE RISK AND COMPLIANCE CONSIDERATIONS

INTRODUCTION

COVID-19 – a tragedy of immense proportions that is having profound impacts on business operations and our interactions with fellow humans. Its ramifications will continue for some considerable time.

In recent years, homeworking trends have ebbed and flowed. Only a short while ago there was a stigma attached to those who worked from home, it was as if they were cheating the company and their colleagues – some people probably were!

Yet within a couple of hectic weeks, we witnessed organisations globally close the door to their business premises and transition to remote working by default. There is very little sign of this reversing any time soon. Indeed a growing number of organisations have stated publicly they are unlikely ever to return to pre-pandemic office occupancy levels.

This paper builds upon a trilogy of papers written by the author, specifically the last in the series[1], and considers upon some of the potential exposures impacting Governance, Risk and Compliance.

GOVERNANCE

As we settle into remote working, management have a responsibility to exercise governance practices to ensure there are appropriate risk assessments, proportionate controls and monitoring in place and that there is transparency and accountability regarding the status of business systems, sensitive information and intellectual property.

Existing corporate governance frameworks, policies and business processes likely require a review and reassessment to identify where they need to more accurately align to the new 'Norm'. Corporate information security policies (business rules) and processes now extend into the home environment and address remote working practices for a much wider audience.

The General Data Protection Regulation (GDPR), with its global reach and implications, stipulates the need for data protection by design and default[2], and for the security of processing (Article 32, 1 (d)) "*a process of regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*".

With the various impacts which involved restructuring how people interact and exchange information, it is important that management can demonstrate governance oversight and evidence that reviews have been undertaken, which in turn will give customers, business partners and regulators some comfort that the house is more likely to be in order.

[1] COVID-19 – Homeworking Privacy & Security – the new 'Norm', 01.05.2020

[2] Article 25 – both at the time of the determination of the means for processing and at the time of processing itself, implement appropriate technical and organisational measures……. in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and to protect the rights of the Data Subject.

RISK

The provision of remote working capabilities for large swathes of the workforce in a very short time has also created a grand scale of potential opportunities for cybercriminals to exploit.

As organisations return to some semblance of normality, there is a need to look beyond the direct human impacts to assess the technical and business risks associated with the long-term operational needs of a remotely dispersed workforce. This will likely influence the associated priorities and capabilities.

Almost overnight video / audio conferencing has become all the rage. Information (i.e. sensitive business financial, personal data and systems technology configurations) is being exchanged often over insecure video and audio feeds. Information, which, in the wrong hands, can be sold on or used for blackmail.

Have rules (policy) for use of conferencing software been defined and disseminated? Are sessions recorded and are all participants aware of this? It is not always clear with some products (beware the unguarded comment). Are there appropriate safeguards for the recordings, how long and where are they retained, who has access to them, are but a few considerations. (IRM can offer further guidance if required).

Remote workers connect to corporate systems via home broadband systems which themselves are often insecure and vulnerable to exploitation. This 'mini home network' in turn, interconnects many other 'uncontrolled' devices, i.e. CCTV systems, utility control systems, televisions, games consoles, other electrical goods (IoT[3]), and family members end-point devices – smart phones, tablets, laptops, etc. – all providing further opportunities for exploitation and routes back to the corporate device.

Have the risks posed by business owned devices being used for 'other purposes' outside their core functionality been considered? This may be to help with children's education, connecting to school, college or university systems. People frequently use work email and password combinations when connecting to online training portals which are themselves potential vectors through which to attack corporate devices.

Where employees use their own personal devices, has there been a risk and impact assessment?

Can employees print business information at home, especially if the output contains sensitive business, personal, financial or systems data, how is this subsequently disposed of?

We are already hearing of significant job losses, though we are unlikely to witness images on mainstream news of people being marched off corporate offices clutching a small box of hastily packed personal possessions. It may be prudent in some situations, when considering the potential loss of data, harm to corporate systems and reputation a departing individual could cause, to inform IT before the individuals who are being let go. Thus enabling some access controls and permissions to be revoked, reducing the risks associated with the removal or unauthorised manipulation of key files, information or systems.

It is important to revoke access to data held in cloud storage systems without undue delay. It may already be too late, some people may have realised what might happen to them, have moved data or changed file extensions to bypass monitoring tools.

[3] Internet of Things – interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data

To reduce risks and help raise security maturity organisations are increasingly turning to thin clients which have many benefits. They require less maintenance, have fewer internal components and need less software, reducing overheads and impacts upon IT Help Desks and support services.

Thin clients are cheaper in the medium to long-term, whilst also being environmentally friendly and energy efficient, consuming less power than traditional PC's and laptops. They are usually more secure as strict policy and hardening controls can be built in and users only permitted access to the servers and data relative to their job role and function. The data does not leave business systems and control.

On the down side, thin clients cannot work without reliable connections to the back-end servers which may require an upgrade to support the increased load and processing activities they need to perform.

Network and server resilience are essential to thin clients being a viable solution. It may be worthwhile considering a hybrid strategy where some functions have thin clients whilst others traditional devices. Conduct a risk assessment to help influence and direct the outcomes and decision making process.

COMPLIANCE

The initial pandemic response rightly focussed on protecting the workforce – keeping people safe. We have weathered the immediate disruption and settled into new ways of working and communicating; but in doing so has there, albeit inadvertently, been a lowering of compliance standards and assurances?

The shift to remote working introduces various considerations regarding the compliance landscape because without appropriate governance, risk assessment, control implementation and monitoring, there is a heightened risk of data breaches and processing contraventions.

Whilst regulators may extend some tolerance and sympathy to lapses in security during the rapid transition to remote working, as time passes, the less they will accept. Aggressive moves to remote working may have created vulnerabilities and exposures that have the potential to be exploited, thereby increasing data protection and cyber security risks.[4]

As management develops and invokes plans to restart and in many instances transform their business, they must not negate their obligations to employ controls that comply with various legal, regulatory and contractual obligations.

A challenge for organisations is to prioritise compliance programmes [i.e. Cyber Essentials Plus, IT Health Checks, PCI DSS, ISO27001, Data Protection, HIPPA, SOC, etc.] whilst balancing reductions in headcount and other associated business costs. Cyber security threats will only continue to increase, they certainly will not evaporate and must not be ignored. Internal and external audits are essential components for compliance and risk reduction. Their activities must be conducted with appropriate rigor in order to provide effective levels of assurance. Remote working may make it harder to audit functions where individuals try to stay off the grid or below the radar, or who work without proper management oversight.

Compliance managers and auditors who adopt a casual approach may be less effective in identifying weaknesses; a greater level of assertiveness may be appropriate. Increased sample sizes might be necessary to provide assurances and verification that controls and standards are implemented and followed correctly by remote workers (who are effectively in mini-offices).

[4] https://securitymagazine.com/articles/92417

Strategically, organisations may opt to place greater reliance upon outsourced security services and partners whose goals must be to provide more risk-based guidance and direction coupled with cost-effective and pragmatic solutions to achieve compliance to the standards and regulations listed above.

OTHER CONSIDERATIONS

AUDIT

To satisfy regulators and attain or maintain certifications, there is a necessity to undertake audits and conduct technical testing. Many audits can still be accomplished remotely; some guidance can be found here – although aimed at ISO9001, the practices and principles can be applied to virtually any standard. The PCI Security Standards Council has also provided a blog for some remote audit considerations; the information can be found here.

Be prepared for some remote audits to take a little longer in order to properly witness and evidence how the controls are being met; having workflows and processes provided to the auditor beforehand can help. Screen captures can provide suitable audit '*evidence*' of the status of system configurations and settings at the time of the audit. Though consider what other information may be available in the screen capture! The user should always provide the image, do not hand over screen control to the auditor.

Recordings of audits (video / audio) including the ownership of the materials, access permissions, subsequent use and retention periods must be confirmed in writing between the parties, and notified to the individuals participating at each stage. Security controls and confidentiality rules apply at all times.

Screen sharing may be appropriate, though take care as to what 'other information' is inadvertently shared, e.g. pop-ups of incoming mail, information available on the device display screen and other materials open in the background.

Agree requirements and processes associated with the audit in advance so as not to incur delays or financial penalties.

Whilst most technical testing can be achieved remotely, this often necessitates installing and configuring software applications on internal system hosts. This is best achieved a few days in advance of the testing and should be facilitated through the organisation's Change Management processes. Factor this into expectations and delivery timescales.

Auditors attest they have conducted an appropriate sample to conclude that governance requirements have been evidenced, controls and processes validated, processes and systems configured and managed in accordance with recognised standards, at a particular moment in time.

Auditors must be diligent and sufficiently thorough to ensure that they are not duped into giving the organisation a false sense of security.

For various reasons, not all audits can be conducted remotely, and measures to facilitate the safety of employees and auditors will be paramount in conducting onsite audit activities in the COVID-19 era.

RESILIENCE

Historically we have focussed on Business Continuity (BC), particularly on internal IT systems and how to cope when they fail. In the world of cloud computing, remote working and online collaboration tools, the emphasis shifts to defining and improving RESILIENCE[5].

Where resilience is considered alongside robust cyber security controls, there are alternate routes and reduced single-points-of-failure (systems and suppliers). Organisations with more mature, resilient and exercised plans prior to the pandemic were more likely to react efficiently and effectively.

An area of resilience that impacted many was the supply chain. In BC 'play books' and scenarios, few organisations focussed on their suppliers. Even where they did, there was unlikely to have been consideration of events affecting virtually the whole world simultaneously.

Aligning, and evidencing operational resilience with cyber security during the recovery, whilst identifying new opportunities, will equip the organisation to add more value to its employees, customers and shareholders.

We are already seeing the threads of a greater emergence towards digital solutions, to move away from the paper-based, manual computing, less reliable and manpowered intensive past.

A CHANGE OF DIRECTION

COVID-19 has accelerated fundamental changes in how organisations will operate in the future. Some of these changes may have been inevitable in the long-term anyway. However, change is being forced at an unprecedented pace and consequently business leaders, management teams and the workforce in general are communicating, collaborating and coordinating on virtual platforms and in ways that few thought possible, or even plausible, only a couple of months ago.

We are unlikely to want to, or be able to, press 'reset' and go back to where we were before.

A Gartner survey (03 April 2020) revealed that of 74% of CFO's surveyed (out of 317), stated the intention to explore the possibility of moving between 5 – 50 percent of their previously on-site workforce to permanent remote working.

Subsequently, more organisations have made similar announcements:

- The Chief Executive of Barclays, Jess Staley, states that "*having thousands of bank workers in big, expensive city offices may be a thing of the past*".
- MasterCard staff can continue working from home until they "*feel comfortable*" about going to the office amid the pandemic. Rather than dictating when they will return, the organisation is allowing individuals to make their own decisions based on their circumstances and needs.
- Twitter, will potentially allow staff to work from home forever if they wish, though for those who desire to return to the office there will be a warm welcome and additional precautions (social distancing measures).
- Mark Zuckerberg, Facebook's Chief Executive, said "*we're going to be the most forward-leaning company on remote working*". The company is looking to aggressively ramp up hiring workers across the USA rather than just those who can commute to its Silicon Valley offices.

[5] Resilience – the capacity and processes through which to recover from adverse situations or change

HUMAN FACTORS

Discussing the human factors could be (perhaps should be) a full whitepaper in its own right. It has to be acknowledged that, for the most part, people reacted reasonably swiftly to the pandemic, supporting the immediate necessities of the lockdown and remote/homeworking – but at what cost?

Whilst some people have been able to quickly embrace the new way of working and will not want to go back to the 'big office' again, there are others for whom this is a personal nightmare. For this latter group particularly, there are mental and physiological issues mounting up, which some organisations seem oblivious to in their rush to use the pandemic as a way to revolutionise and change how they conduct future business – "*everyone can just work from home*" just does not cut it.

Organisations are required to conduct Risk and Health & Safety assessments[6] of all activities conducted by their workforce, and they now have multiple new locations to assess. Some people are not fortunate enough to have their own 'office' space, but share or even compete with other family members for access to computers, network bandwidth and privacy to conduct work activities.

Has remote workers insurance been considered? Will employees' contracts and terms need revising? Are there appropriate technologies and business policies? A number of factors to consider can be found here.

The Institute of Workplace and Facilities Management[7] conducted a survey of 2,200 people in which only one in four said they had a separate office, most said they use makeshift workstations on dining room tables, sofas and beds. Flatmates, family members can be just as disruptive as noisy workplaces. Many offices incorporate zones to facilitate different types of working – quiet rooms for concentration, open spaces for collaboration and social interaction; such luxuries will not exist in many homes. What happens to the office banter and the team dynamic when everyone is dispersed to far flung locations?

For many people, working from home as an emergency response to help prevent becoming infected or spreading the pandemic is one thing, working there permanently is a different proposition. Like in many aspects of life, one size does not fit all, every individual's circumstances and needs are different and it will be a complex issue to resolve and will necessitate effective communications.

Of course economic circumstances, business and individual, will influence decisions, particularly in the short-term. It will not be easy for many employees to consider alternatives given the likely state of the job market. Maintaining income stability will be vitally important, but how will the organisation further motivate and incentivise their people in the short, medium and longer term?

CONCLUSIONS

Inadvertently perhaps, the pandemic brought forward transformational change by 7-10 years. We were initially caught out by the magnitude and pace of its impacts to our business and personal lives.

Not all decisions made by governments or organisations as a consequence of their response to the pandemic are popular; yet they will have a profound and lasting impact upon its people.

History from previous pandemics shows that we will find new ways to operate, to conduct business and to regain a sense of a 'new Norm'. Many things will undoubtedly be different. In the last couple of months we have witnessed phenomenal growth and dependency on digitisation, which will likely continue apace for the foreseeable future.

[6] Management of Health and Safety at Work Regulations 1993

[7] https://www.iwfm.org.uk/

As businesses change their operating models, many big office spaces may become surplus to requirements, employees will alter their household layouts to facilitate permanent changes to their work-life balance.

Irrespective of the direction in which organisations head, appropriate and proportionate steps must be taken to continue to safeguard the organisation's technology systems and information assets.

Security and Privacy by Design[8] are as important now as ever, particularly as there are now many additional dispersed end-points to control, safeguard, monitor and manage.

Businesses will need to consider the impacts and requirements to demonstrate good governance, to reassess and evaluate their cyber security and data risks, whilst assuring compliance with ever-growing legal, regulatory and contractual obligations.

When doing all the important things to maintain privacy and security, organisations should not neglect their most important asset of all – the humans who make it all work and on whom you depend so much – take them for granted at your peril!

> *"Everything we do before a pandemic will seem alarmist.*
>
> *Everything we do after a pandemic will seem inadequate."*[9]

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)" –** provides organisations practical advice and guidance in their preparations:

https://www.irmsecurity.com/resources/practical-pandemic-planning-p3-coronavirus-COVID-19/

- **"COVID-19 – Data Protection & Cyber Security"** – addresses some considerations pertaining to data protection, remote working and human factors:

https://www.irmsecurity.com/resources/covid-19-data-protection-cybersecurity/

- **"COVID-19 – Homeworking – Privacy & Security - the 'new Norm' –** promoting various thoughts and posing questions that organisations' may have overlooked or may need to revisit: https://www.irmsecurity.com/resources/covid-19-homeworking-privacy-security-paper/

[8] GDPR Article 25 – a mandatory requirement to "implement appropriate technical and organisational measures

[9] Mike Leavitt – former US Department of Health and Human Services