Back to 'Normal' Proceedings at Work

– Maintaining (Operational) Security

QUOD ORBIS

Re-evaluating working processes and operations

During these challenging times, organisations have had to re-evaluate their working processes and operations. In most cases, this would have included remote working with the assurance over how this capability is provided and utilised (please refer to the previous paper: Remote Working During Critical Times - The Assurance That Organisations Need to Have and Provide).

With this in mind, organisations' horizon planning must also account for when normal proceedings, or an attempt to attain such, ensues. Therefore, questions over the state of considerations such as readiness, operational requirements and their security will be even more pertinent. This is to ensure a smooth transition, from what may have been a reduced and skeleton crew approach, to full operational activity.

So, what does this mean? Are organisations ready to return to pre-Coronavirus operations and activity? What do organisations need to ensure that returning to such a state does not become a detrimental venture? This paper highlights some key points and areas to consider when such an option becomes a tangible reality.

Bring Your Own Device (BYOD)

It would not be surprising to see that the increase in remote working has brought on the proliferation of personal devices being utilised for work purposes. With the return to work, organisations should review their policies and controls based around the use of personal devices and decide if the continued use of such is compliant with the prevalent security mandates and requirements. Personal devices afford a higher level of control to their owner which subsequently translates as avenues for misuse of company intellectual property and resources if not managed accordingly.

Considerations for organisations

Hygiene

In addition to the point concerning BYOD, organisations will need to review the configuration of the remote connected devices. Compliance to defined build standards will be a key requirement here. This will include looking out for any instances of shadow IT, non approved software and hardware. A network access control solution can be employed to ensure that any devices joining the corporate environment are configured to only utilise company approved software and hardware. This is especially pertinent as non approved items introduce a greater risk of security attacks and breaches.

Compliance Requirements

Organisations will need to ensure that for the regulation or framework upon which successful continuation of their business is dependent on, the environment is conducive in maintaining the necessary compliance. With the current crisis, disruption to compliance adherence can well be expected as efforts will be focussed on the key aspects of the business. However, upon resumption of normal operations, such reduced observations of compliance to regulations and frameworks will manifest itself as areas of compromise. As such, it will be of great importance that any compliance shortfalls are identified and addressed. This aspect is made easier for organisations by use of an automated platform to assess the existing controls. By this, organisations will obtain an unbiased true reflection of the status of readiness for normal proceedings and operations. Organisations will also be provided with a measurement against their success in these attributes and their compliance requirements.

Training

In the absence of physical interaction with staff members and immersion in office culture, observance of security requirements and general security awareness may lapse. Not being constantly reminded of employee security responsibilities, be it as posters, town hall meetings or general inclusive awareness campaigns, can result in employees neglecting to adhere to their organisation's security policies and awareness mandates. Organisations will need to undergo an extensive security awareness campaign to help ensure that their employees maintain to improve upon their security posture. This will help reduce the employee introduction of threats and potential security breaches.

Permission / Access levels

Access levels for employees may well have been revised to accommodate for the current crisis restrictions. Instances of emergency and escalated access and permission levels may have been granted to ensure the continuation of operations. This measure, although with the intention of being temporary in nature, often extends well beyond the time period for which it was intended. Organisations should audit their users for relevance of the role performed, the access requirements and the permission levels granted in terms of applicability and necessity. All too often we see cases where, under extreme circumstances, the permission and access levels are escalated only for them to be retained long after their need has passed. Retaining increased levels of access, permission and privilege beyond what is necessary is conducive to the introduction of threats and attacks.

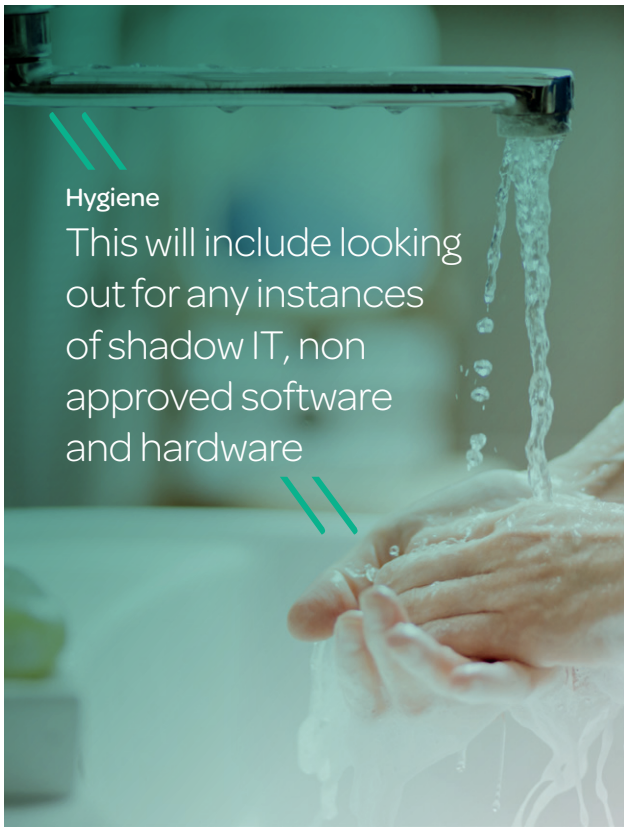
Monitoring

Operational hours during the remote working period will most likely have not followed the traditional pattern of the organisation. These working hours and what may appear to be erratic access occurrences will need to be monitored as return to some sense of normality takes place. Essentially, odd working hours should thus no longer necessarily be the norm. Therefore, corporate access outside of what is to be expected will need to be alerted for and investigated to determine if such activity is required or suspicious. However, with the possible introduction of staggered working, the related access activity will need to be factored into organisations' monitoring services.

Physical Data

Data in its physical form may have been kept outside the organisation's office locations at the homes of employees. This is an important point to consider as, when employees return to their places of work, organisations will need to decide whether these documents must be returned or if they should be destroyed at the employee's home.

As more people are working from home, this thought process also extends to home printing where pertinent company data is physically reproduced. Clear instruction over their retention, disposal and destruction must be communicated to employees. This can be supported by implementing data leakage prevention to ensure that personally identifiable information and / or company sensitive information is not being printed. Additionally, limiting who can print sensitive documents will factor in the security over high value company data.



Back to 'Normal' Proceedings at Work

– Maintaining (Operational) Security

Flexible working

As it is expected that more people will be working remotely, security around the provision of this service must be employed. This encompasses company and personal devices solely for employee use, licensing requirements, automation where possible, secured connectivity, company approved solutions, effective monitoring and assessments, strong support of IT services as well as robust authentication, authorisation and accountability. The earlier paper, Remote Working During Critical Times - The Assurance That Organisations Need to Have and Provide, expands on these points to provide further information on the best practises that organisations can employ to help reduce the consequential breaches and attacks.

Scalability

Organisations that enable their systems' ability to handle a growing amount of work by adding the required resources will be better prepared for future high impact events. As such, organisations should get ready for future events of disruption as, for example, it is not unreasonable to envisage that this type of pandemic will occur again. Therefore, increased virtualisation with the ability to scale out as required, investing in a strong crisis management function and providing secure remote working, will help organisations to be better prepared for the return to full or near full operations.

Response plans

With the return to normal operations, the physical organisations' locations of activity will most likely be emptier than before. Consequently, organisations should concentrate on ensuring the security of the information and equipment located at their physical premises. Response plans encompassing undesired events such as incidents and breaches will need to be assessed for their aptness and relevance. One example of which being: what if the personnel dealing with an incident or a breach are unable to physically stay together in the same designated room?

Insider threats

Downsizing in response to the current climate will be an unfortunate reality for some organisations. With this may come loss of work for some employees or undesired changes to previous employment terms and conditions. Such changes may result in staff becoming disgruntled with their situation. This then increases the risk of compromise to organisations via nefarious practises by their staff as an expression of their dissatisfaction. Organisations will need to consider the risk of these insider threats and the required monitoring, alerting and mitigations in order to protect their assets.

Organisations will benefit from a one stop approach to identifying and understanding their readiness to return to normal operations following the aftermath of this crisis. By analysing their current status, the issues and their remediation can be determined. Quod Orbis provides organisations with an unbiased and accurate reflection of how well prepared they are for the return to normal proceedings and operations through the Quod Orbis Controls Platform. The Quod Orbis Controls Platform provides a measurement of how successful companies are in their readiness for resumption to normal services with metrics against their risk, cybersecurity, regulatory and compliance requirements. For further information on how Quod Orbis and the Quod Orbis Controls Platform can assist your business in assessing operational readiness, security posture and compliance maintenance, please reach out to us at contact@quodorbis.com.

Stay safe, stay productive.

QUOD ORBIS

About Quod Orbis

Quod Orbis is team of cybersecurity experts leading the way in the latest evolution of enterprise risk and security for organisations worldwide. Quod Orbis uses a blend of consultancy and services to identify and manage digital risk for clients across Financial Services, Large Corporations to Governments and household brands. Quod Orbis helps organisations identify risks and fix the issues with a clear and simple definition of the problem and delivery against prioritised end goals. With this no-nonsense approach, the hype and noise are cut through to help with the transformation and security of your business with complete peace of mind.

Get in touch

If you would like to speak to an expert about protecting your business, get in touch today.

33rd Floor, 286 Euston Road (Euston Tower), London, NW1 3DP, UK

+44 (0) 203 9622206

contact@quodorbis.com

quodorbis.com