REDLEAF CONSULTANCY
A SECURITY PRACTICE

Covid-19: A Change in Context that Might Affect Controls in a Risk Environment

Covid-19 – Losing Control

The seemingly temporary measures introduced because of Covid-19 are taking on a permanency that may not have been foreseen. This is particularly focussed on homeworking, but that cannot be allowed to mask the effects that it is having on the wider risk environment, together with the controls and context in which the original pre-pandemic decisions were made.

When Covid-19 struck, few people could have foreseen the impact that it would have on business or society at large. The initial rush of grabbing PCs, taking files from cupboards and setting up home offices has passed and what was maybe seen as a temporary measure, has developed into one that appears to have a permanency about it.

The return to places of work, when it does happen, will not see business as usual. As employers implement Covid-19 protective measures, there will be changing patterns in work activity, a reduction in staff numbers within buildings and a continued preference for homeworking. While Covid-19 is the current predominant threat, it has, at best, only masked the threats that were there prior to its arrival, those threats are active now and in the current climate probably seeking to exploit new security weaknesses. However, those weaknesses may not be to do with the physical security features that there are, but the context in which the original risks were identified, controls established and the impact that might have on risk governance.

As businesses move forward and develop new plans that might see an increased focus on resilience, the disposal of property or the reimagining of offices, there will be an obvious time lag between the inception of those plans and their final delivery. Through that change period it is critical that the risk management process, in all its phases remains effective, with assumptions not being made.

Within an effective security regime, the establishment of the security risk in its simplest form is modelled through an equation:

Risk = Threat x Vulnerability x Impact

In itself the equation does provide guidance on the how the risk is to be mitigated through the use of controls, including those that are physical and procedural, but it does not bring that within a governance regime. The controls that were introduced have to be seen to be effective not only in light of a dynamic threat environment but in response to business operations and governance, amongst other things, does that.

In operational terms, the way businesses operate now is not the same as pre-Covid-19, not least of all because of homeworking. The protection of information, for example, is not only dependent on cyber security, but physical security controls, which are normally adopted within an office environment, but which are not available at home.

Maintaining controls that are maybe obsolete and which were set in the context of a different business climate may no longer reflect current needs. Without review and taking into account business operations, within a Covid-19 environment, increases the danger that the threats that there are will expose the vulnerabilities that have arisen.

If security is taken as a one-dimensional function it may, for example, see its role as purely responsible for installing equipment or providing security officers in direct response to threat actors seeking to exploit vulnerabilities. Even if KPIs and SLAs are monitored, without a true evaluation and extrapolation of information from the controls and in light of operational practices, the effect that security has on mitigating the risk will not be known.

Security is a risk-based function, in that it has to understand the degree to which a wide spectrum of threat actors might prevent a business from delivering its objectives. Through understanding the impacts that would be made, should the threat be realised, and working within a predetermined risk appetite, a series of controls are established that mitigate the risk.

The controls can be any measure, whether that is; procedures, training or the installation of equipment, but those measures are not independent but integrated to provide the overall control. In a one-dimensional security environment, identity cards, for example, are seen as a method of identifying who people are and which group they belong to, whether that is permanent staff, contractors or visitors.

However, as a control on an identified risk, including the loss of information, different coloured identity cards for each of the groups indicates who, for instance has physical access to information or critical infrastructure.

Taking a metric on the number of forgotten identity cards provides limited information, however by extrapolating that into perhaps the age groups that people fall into or if the there is a prevalence amongst staff in a particular department who forget their cards, that is useful.

It can be taken as a leading indicator that if staff cannot remember their identity cards, what does it say about the general application and culture of security in that department? It is this type of analysis, across the range of risks that there are and the controls in place, which enables effective governance, when taking into account fluctuating threats and operational requirements.

However, if the controls were established prior to Covid-19 and have not been reviewed in light of that, there is a danger they may not be mitigating the risk as expected. The context in which those controls were established has changed.

Taking a position that there have been no incidents does not mean that security is good, it just means that nothing has happened, for whatever reason. There has to be ongoing analysis, across the range of risks that there are and delivering a product to individual risk managers on how, through analysis, the effectiveness of controls is delivering that.

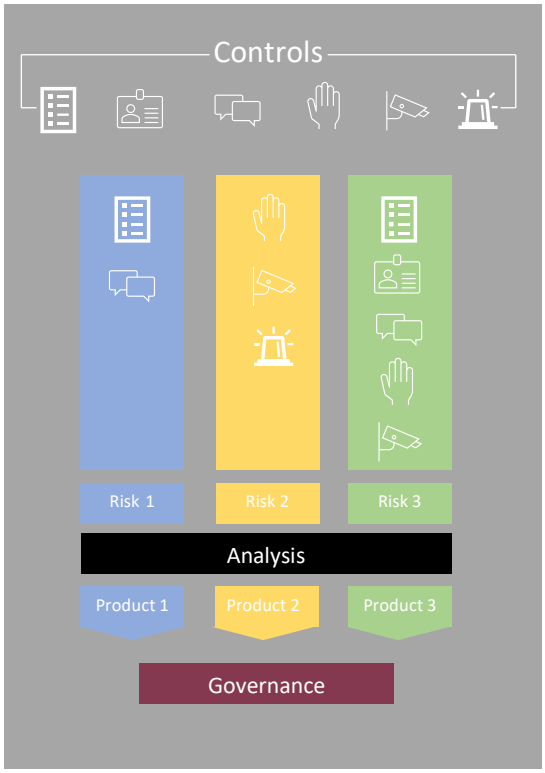
Covid-19 has probably changed the context in which original decisions were made and this could have a direct bearing on the ability of the controls to mitigate the risk

Although security can appear monolithic, it should only be responding to business risks that are possibly owned by operational line managers. The diagram opposite illustrates how individual controls are used to modify the spread of risks, but as can be seen that while security might provide a range of controls, they are specifically targeted towards individual risks. It is the role of security to work with the risk owner to understand not only the risk that is being mitigated, but the specific threats and operational processes that might affect it.

Throughout the life of individual risks, security has an ongoing responsibility to analyse how the controls are functioning in light of the threat and operational needs of the risk owner. Periodic and predictive reports are required that should be tailored into specific products that meet the needs of individual risk owners and it is this which enables confidence in a governance regime.

Clearly since Covid-19 the context in which risks decisions were made has changed. The context is not only the business objectives and how they were going to be achieved but life more generally. The pandemic has changed that context, it has driven the way people work, the services that support them, how shopping is done and where they get their morning coffee from. The certainties and context that led to establishing the risks prior to Covid-19 has changed and there is a need to adapt.

There is an understandable focus on homeworking and the controls surrounding that, but that should not be allowed to override the other risks that there are. The loss of a data centre or other critical infrastructure on which a business depends, the theft of high value items or the impact of terrorism, could have a serious impact on a business's ability to operate, in an environment where issues are being compounded by the difficulties surrounding Covid-19.



It is the case however, that controls which were implemented pre-Covid-19, should not be abandoned or altered without understanding what the impact on risk would be. In the current climate when hands free technology is seen as a protective measure, the use of mobile phones might negate the need to touch an access control reader, but if that leads to identity cards no longer being used what other what other controls are going to put in their place, how are leading indicators going to he arrived and what impact will that have on monitoring risk within a governance regime?

Operations have changed but there is a continued need to address the risks across the business

While plans might be being made on how to reoccupy buildings and bring businesses back into operation, as a concurrent activity there is an immediate need to evaluate existing controls. All procedures, should be reviewed to ensure that they are practical and do not cause delays where senior managers, for example, may no longer be in the building.

The context of the new environment has to be examined and that might alter the ability of any of the controls to modify the risk. This can only be done by understanding how business operations are functioning in the new climate and if that has developed new vulnerabilities, which could be exploited.

Ensure that within a governance regime that the analysis of data from the controls and other sources actually reflects the risks that are being mitigated. If working practices have increased vulnerabilities and controls have not been altered the impact of that should be reported to those individuals who are responsible for managing risk.

This is not a simple process and it is time consuming, but as circumstances changed, security must adapt and project the risk on decisions being made.

The effect of introducing new measures has to be understood, to ensure they do not conflict with existing controls

Aidan Anderson, of RedLeaf Consultancy, is a Chartered Security Professional, who has acted both as a Regional and Group Security manager for a High Street bank. He established security within the Bank's risk management framework and dealt with the serious operational difficulties in Northern Ireland of terrorism, kidnapping and robbery. A keen advocate of security being seen as a risk-based process, set within a governance regime, Aidan can be contacted by:

Mobile: +44 7720 820023
Email: aidan@redleafconsultancy.co.uk
Web: www.releafconsultancy.co.uk