REDLEAF CONSULTANCY
A SECURITY PRACTICE

Covid-19: The Difficulties of Cost Cutting in a Secure Environment

The economic impact Covid-19 is having is not difficult to see, as daily new announcements are made on job losses from aerospace industries to sandwich shops. Behind the redundancies, businesses are restructuring, setting new objectives and engaging in cost reduction measures in a bid to survive for the long term, however the objective, from a security perspective is to maintain a secure organisation.

The Difficulties of Cost Cutting

In any business environment, there is always a downward pressure on costs, which is normally experienced during the annual cycle of budget preparations. Within the current operating climate and the graphic impact that Covid-19 is having that downward pressure is being felt now.

The severe effect of the pandemic may well magnify the issues of the services that are supported, and the investments made by businesses, who will challenge internal departments, including Security, on their individual running costs and staffing levels. Some security costs, particularly those that see the disposal of property will occur as part of larger planning, but others within the immediate Security realm will require difficult decisions.

Whether the cost challenge is given as a straight fall in terms of available cash, as a percentage of overall spend or as a reduction in staffing levels, it will require a review of the services provided by Security.

Although the challenge is there and must be met, Security is a risk-based function whose future operating plans should be based on a risk judgement rather than just an arbitrary cut. Clearly all internal departments will be justifying their expenditure and perhaps seeking more in light of new business models. It is up to a business where expenditure is made, but without a logical argument that overcomes assumptions being made by some decision makers, Security will be less likely to succeed in its primary objective.

The objective of this paper is to provide a view on how Security, operating within a risk environment, might meet the difficulties being encountered. Seeing Risk as a series of annotations on a Heat Map is wrong, but rather it should be the outworking's of detailed analysis and a verifiable process that withstands examination. It should set out for those ultimately responsible for managing the risk, with the information they need to make decisions that reflect their priorities.

Security has to move with the Business it supports and accept the challenges that there are. It will require an understanding of what the changes might mean for the objectives and structure of a business, how new or emerging threats will react to that and the exploitation of vulnerabilities that might be generated through those changes.

Understand the Changes and Objectives

Within the security environment, it is normal to see statements such as, *Security must align itself with the business's objectives.* Although this is true, as those objectives are cascaded down, individual departments have to organise themselves and set their own objectives to meet overall business aims. Structural changes, cost reductions and new objectives, may well affect how departments function and alter their individual risk profile, including the impact security has on that risk.

As a function, Security not only has to understand how any new profile will affect individual departments but enable the appropriate security structure to put around it. One of the reasons for this is that Security is not just about protecting the business as a whole, but individual departments and project teams within it, who carry and treat their own risks.

Effectively, Security should be providing a tailored product that meets the individual risks that departments have, but as operational changes are made, those departments have to be engaged to establish what it means for their risk profile. Those changes might mean a variance in the level of security controls needed, but that would have to be understood to enable the security element of that risk to be established.

Realising the Threat

The degree to which any business is under threat is fluid and not only varies with time and geography, but how it attracts threats through the objectives it has, how it is structured and at present, the way in which it is responding to the ongoing and post Covid-19 environment. Taking a generic threat assessment, without analysis and understanding of how any threat actors might exploit structural or other changes in the business, runs the danger of either over or underestimating the potential issues that there are.

Understanding the threat, as it currently exists is beneficial but limited, as any decisions being made are for the longer not the more immediate term.

From analysing the Threats and understanding the Vulnerabilities there are, will lead to the Impacts there, should the threat be realised. However, Security is a product that the business has to buy and like all products in must not only meet the needs of the customer but be within cost.

Therefore, the production of a threat assessment should not only be timely and accurate but be predictive and aligned to the business. The threat actors that were there prior to Covid-19 are still there, while in addition others might have emerged. To gain a full picture will necessitate a comprehensive review of the threat landscape, as it relates to the business.

Establishing the Vulnerabilities

Vulnerabilities are often discussed as weaknesses within physical security systems or procedures, as they counter the expected threat. However internal changes in an organisation can generate greater if unintended consequences.

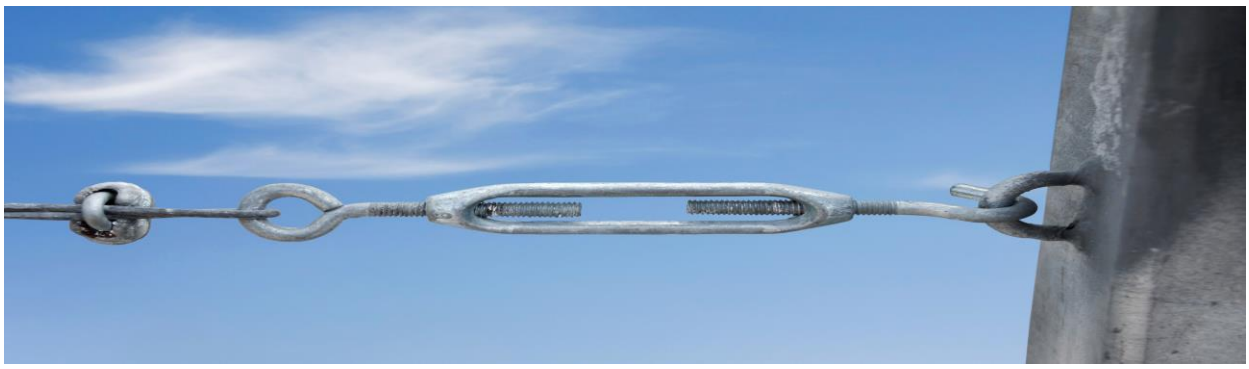
The consolidation of business units could mean, for example, that the reporting line of Security changes. If security is seen as an ancillary function and not integral to the business that might not be a problem, however if it is, issues can be generated. The filter that can happen if Security is a small part of a larger department, who are not risk orientated, could lead to a dilution of both influence and the independence necessary in delivering an effective security product.

Providing that the regular cycle of reporting within a governance regime has been undertaken, the vulnerabilities that existed prior to Covid-19 should be known about and re-assessed against the projected threat. If that base knowledge does not exist, it should, if time permits, to be physically gained. If time does not permit, it will still require a desk top review that should be collaborative and draw on the knowledge people have.

Charting the Impact

Through evaluation of the Threat, combined with ongoing analysis of the Vulnerabilities that exist the Impact that would be made, if the threat was realised, would be understood. This will set out in a logical format the relative criticality of the risks being managed and take into account the risk appetite that a business has, whether that is measured in quantitative or qualitative terms.

The process will grade individual risks and enable the direction of resources to those that would cause the most damage. It will facilitate the introduction of measures to mitigate the risk.



Implementing cost reductions and staff redundancies is never easy, it is at the end of day people's livelihoods that are at stake. However, Covid-19 is affecting business survival and while difficult decisions will have to be made, they should be done so following extensive research, planning and focussing on long term business needs.

Delivering a Product

Security is a product that the business has to buy and like all products it must meet the customer's needs, aspirations and budget. There is little point in producing a product that the business cannot afford, it has to be brought within the available spend and this is the challenge posed by budget and staffing reductions. The only way to know what internal customers needs are is to speak to them and to design the product around that in light of the known risk.

Security officers, CCTV cameras or even security surveys are features within the product, it is the benefit to the business that is where value is derived. The overriding benefit, is that security enables the business to achieve its objectives.

Through understanding the Impact that would be made, if the threat was realised, should provide guidance on what features are necessary to enable delivery of the product. In some cases, this might require a paradigm shift, with Security perhaps only undertaking high value add work. However, minds must not be closed to new ideas or ways or working just because it hasn't been done before, proposals should at least be evaluated.

It is maybe too soon to know if the changes brought about by Covid-19, whether working from home or the use of small and agile project teams will be permanent, but Security must adapt to the new landscape. The product it produces must be geared to the needs and expectations of the business as a whole, individual departments and project teams and brought within the level of available spend.

If not already done so, Security should have a place within the Governance regime to ensure that there is both accountability and responsibility, as well as to ensure that the compliance and foresight necessary in Security Management, is being recognised and acted upon. This will enable senior management to see the function that Security performs and the benefits it brings.

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