REDLEAF CONSULTANCY
A SECURITY PRACTICE

Security – The Road to Resilience

RedLeaf Consultancy

Phone: +44 7720 820023 Email: info@redleafconsultancy.co.uk Visit: www.redleafconsultancy.co.uk

Security – The Road to Resilience

Resilience, in terms set out by the UK Financial Conduct Authority is the ability to prevent, adapt, respond to, recover and learn from operational disruptions, and is critical to all organisations, not just those in finance. The current pandemic might have brought Resilience to the fore, but even without that, in an interconnected world and with numerous interdependencies, it and Security's place within the solution, is perhaps more important than ever.

Resilience is an inherent human characteristic that enables people to adapt and change and ultimately move forward despite prevailing conditions. As a business concept, Resilience has become increasingly formalised and accepted over the last 40 years, with significant events, such as the Great Financial Crash (GFC) of 2007-09, giving it increased acceptance and impetus.

With the wide-ranging effects that the GFC had it is perhaps not surprising the financial sector and the critical dependence that the economy has on it are pushing the agenda. This is seen through the:

- UK Financial Conduct Authority, (FCA), who, together with the Prudential Regulation Authority and the Bank of England, published a policy statement in March 2021, PS21/3 *Building Operational Resilience.* The policy, which comes into effect in March 2022, is designed to ensure that the financial sector can protect their *important business services* from disruption.
- Basel Committee on Bank Supervision, (BCBS), set out in their March 2021 policy document, *Principles of Operational Resilience,* a list of 7 Principles ranging from governance to interconnectedness to 3rd party dependency management.

But it is not just the financial sector who are pushing the Resilience agenda. The UK Government is looking towards Critical Infrastructure Resilience and are seeking evidence as part of their review into that with the final results expected in March 2022.

On one level there is a natural concentration on systemically important services, whose loss or disruption could have a serious impact across multiple sectors. However, Resilience is important to all organisations, where it is an enterprise-wide issue.

Creating a Resilient organisation is not just limited to Security, but through the process, there is a tendency to concentrate on Cybersecurity. Cyber is a critical area and reflects the dependency all organisations have on it, but Security more generally, is essential in building Resilience.

This can be seen on a daily basis whether it is, through the disposal of property and the concentration of key functions into a reduced number of sites, data centres, particularly if they are outsourced or even the ports that are relied on for the import and export of goods. Their loss or serious disruption could negatively affect the Resilience of any organisation, without having compromised a single bit or a byte.

While Defence in Depth does provide solidity, it can be seen as a monolithic structure, with hidden cracks and fissures, which without constant examination could go unnoticed, until there is a catastrophic failure.

Twenty-Twenty Hindsight

With hindsight it can be incredibly easy to understand why some organisations have an ability to adapt and survive, while others don't. Organisations are as individual as the people within them who have different views and life experiences all of which forms their opinion on the direction to be taken.

However, catastrophic failures are rarely caused by a single issue, but rather multiple issues which when compounded and put under stress, trigger's the crisis. Even within Security and while *Defence in Depth* does provide solidity, it can be seen as a monolithic structure with hidden cracks and fissures, which without constant examination could go unnoticed, until severely tested. In themselves Security failures have to be seen in a wider organisational context and the place Security has within it, rather than purely systems, whether those are physical or procedural.

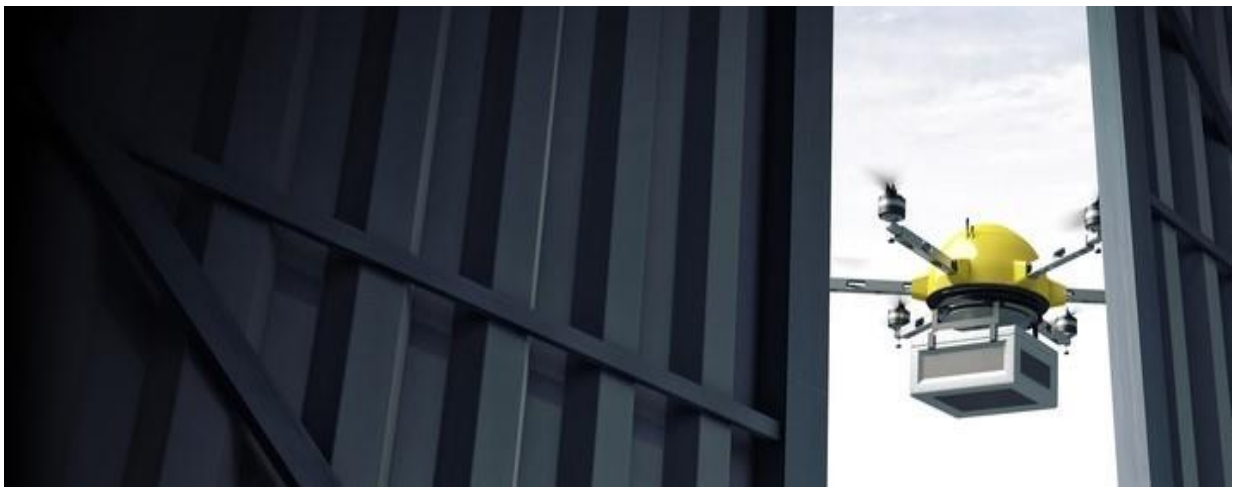
Most Threats will be known about, what might be missing is an appreciation on their immediacy and impact

Managing Risk

The foundation of Organisational Resilience is understanding the Risks there are. However if Security is only seen as a function that protects physical assets, whether it's the buildings people work in or the high value goods they might contain, then perhaps it is being looked at from the wrong perspective.

For Security to have an effective role in Resilience, it has to be seen as a Risk based function which understands what it is that an organisation delivers and how it is being delivered. It is through that analysis which will enable the most appropriate mitigation strategies and controls to be put in place.

Although Security might own some elements of Risk, it is maybe more likely that it is providing analysis to other risk owners, across an organisation. It is up to Security to actively engage with those risk owners, to provide analysis on their individual risks and from that establish a composite picture on the cross-organisation security issues there are, including the dependency of critical departments on nodes which might have been unknown or their importance not realised.



The Unexpected – Building Capacity

However, developing resilience on expected risks does not allow for unexpected events which could overwhelm any defensive measures. Reserve capacity should be built, but this does not solely relate to physical controls, which in any case are not impermeable. It relates as much to the capacity that the security team has as a whole, from the security officer to the security manager and their ability to work effectively in difficult and unusual circumstances.

It can only be created by challenging the team, putting them into difficult but controlled situations, from which they can learn, grow in their capacity and to be ready for any out of the park event. This includes the ability for local teams to take control and make decisions should it become necessary. It is very difficult sitting thousands or even hundreds of miles away and remotely trying to manage response and resources on the ground.

Developing The Intelligence Picture

Resilience is often captured in terms of Black Swan events or the unknown unknowns, but most threats will be known about, what might be missing is an of appreciation on their immediacy and impact.

Reading a newspaper, attending a conference or subscribing to threat intelligence services, is useful, but limited in providing a complete picture. In itself the production of intelligence should not only be organisation specific but achieved through the systematic exploitation of a range of sources which when analysed provides a product that is not only forward looking but which enables decisions to be made.

However any assessment should not be limited to the organisation itself, if there are critical dependencies, the threats which bear on them are just as likely to impact the organisation and must be explored.

The Intelligence Picture is not solely for the use of the Security Team, it is a product that enables decisions to be made at a Strategic, Tactical and Operational level, depending on the target audience.

Failures can build up and maybe even go unnoticed until they cause a catastrophic event or result in an inability to react

To provide the correct picture at the correct level, the intelligence product, or Threat Assessment, has to be tailored towards individual needs. After all the needs of the Board and the global view they take is different from the near-term hazards of a local operations manager.

However, having a forward-looking assessment and which scans the horizon, is not the same as having actions carried out on its contents, but it should feed back into the collective and individual risk assessments. This will allow an appreciation of the impact that fluctuating threats has on the risks that there are and for the risk owners to make decisions on those actions to be taken.

Capitalising on Failure

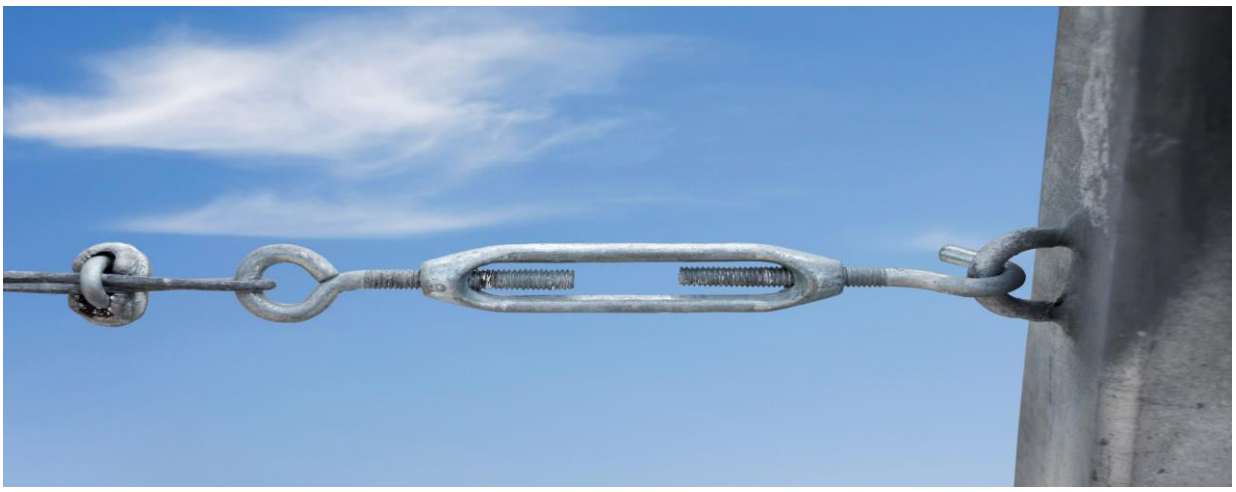
Failure is not restricted to an event that overtly breaches security protocols and which results in loss. There are probably failures every day that are caused by instructions not being followed, people feeling unable to challenge the status quo or just by them simply being unaware or uninterested, but that don't result in immediate loss. However, those failures can build up and maybe even go unnoticed until they cause a catastrophic event or result in an inability to react.

Understanding where daily failures occur can only be achieved with engagement and encouraging feedback from all staff, not just those in security. Capturing data from the security devices that there are, which through analysis and extrapolation can provide leading indicators on potential issues.

Data Sources – They Probably Exist

If, for example, the only information taken from intruder alarm systems is data on false alarms and how to reduce their incidence, this does not capitalise on the vast amount of information that each sensor produces. Even when the alarm is switched off, it will produce patterns of activity on daily use that will enable potential failures to be identified at an early stage.

Security issues are not the only business interruption factors that will challenge an organisations resilience



Challenging Accepted Practice

Security, perhaps like most professions can live in an echo chamber, people come from similar backgrounds, undertake similar roles and attend similar courses. On one level this is reasonable, as it allows good practice to be disseminated and maybe provides an understanding of what the latest threats are, but it can be a drag on challenging accepted practice, who wants to be the first to do something different?

But Security should be challenged, open to being questioned and accepting of new ideas from all sources. Without that there is likely to be only incremental change, rather than maybe the seismic changes needed to ensure Security's and the organisations survivability.

An Uncertain Future

Security issues are not the only business interruption factors that will challenge an organisations resilience, but it is likely that whatever the challenges security will be affected. In itself the current pandemic is not a security issue, but the effect that it has had and the way in which organisations have dealt with it, has altered security risk profiles, whether that is because of working from home or even the changing patterns of activity on which operational security is based.

Whether Resilience is being adopted because of regulatory pressure or as part of organisational good practice, the process not only has to start with understanding the Risks there are, but what existing measures are in place and which could be exploited.

As with any journey the Road to Resilience requires planning, with some of the directions set out in this document. It is however a journey that has to be continuously re-evaluated and altered as the path changes.

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.redleafconsultancy.co.uk