RedLeaf Consultancy
A Security Practice

The Case for Merging Physical and Cyber Security – Has it Been Made?

www.redleafconsultancy.co.uk

There are calls for Physical and Cyber Security to be merged to fight what is seen as a common threat. However is their merger warranted and would it work?

Introduction

The advance of digital technology, not only in business but in everyday life, is a key component of the early 21st century. As technology becomes ubiquitous within every facet of life, access being gained to networks through smart phones and tablets and with growing demand for cloud computing and software as a service, the possibility of compromise increases.

Whether it's the theft of information, damage to systems or reputation, the cyber threat is real and of national concern. In November 2011, the UK government published its Cyber Strategy, which not only recognised the substantial benefits of the digital age, but saw the threats that existed and which could, if not controlled, prevent delivery of the very benefits envisaged.

Such is the projected threat that cyber security has been recognised by the UK government as a Tier 1 threat. This top level threat sits alongside international and domestic terrorism, major accidents or natural hazards that necessitates a national response, and an international military crisis that draws in the UK and its allies. The cyber threat is not just at national level but affects businesses and people as they go about their daily lives.

Dealing with cybercrime requires a multiagency response and it is perhaps because of this there is a vision of cyber and physical security merging. Both fields, in general terms, have a common goal – to protect an organisations assets. But can two disparate fields add significant value by being merged or is their strength found in being apart.

Cyber Security is marked out as a Tier 1 threat by the UK Government, but risks to businesses do vary and while Cyber is an important issue, it has to sit beside all other risks

Risk in Context

In itself the threat posed by cybercrime is not new. The targets are the same, whether that is about stealing intellectual property, gaining access to classified information or sabotaging critical infrastructure. What has changed is the frequency of attacks, the spread that there is across an expansive range of organisations and people, when combined with the ability of an attacker to sit remotely, undetectable and it would appear risk free. But cyber is not the only risk that an organisation faces and while it is a UK Tier 1 national threat that may not be the same for all businesses.

What is known about risk is that it is not restricted to a single vector and in the case of Financial Institutions (FIs) operating in the United States, non-compliance resulted in American regulators fining FIs a total of USD53bn in 2013 (*Financial Times*). According to statistics from *Oceans Beyond Piracy* the estimated cost of the effects of piracy off the Somali coast in 2013 was USD3.2bn. Even what might be termed as single one off crimes such as the kidnapping and robbery at the Securitas cash centre in Tonbridge, England in February 2006 resulted in a loss of GBP53m (approximately USD94m).

Risk is of course not just a figure, it is a process that allows organisations to understand potential issues that can, if not recognised and treated within their risk appetite, could affect the delivery of strategic goals. Whether those risks are generated through regulatory noncompliance, the perils of Somali pirates or kidnapping gangs, Cyber and Physical security are just two more business risks that have to be treated within an organisations Risk Management Framework.

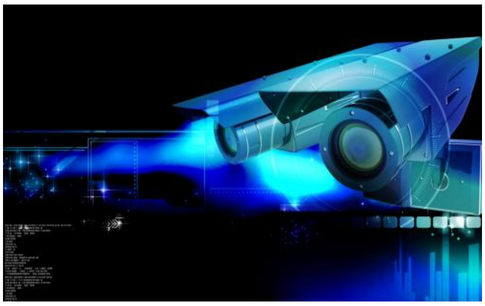
The Threat

To a large degree the block of people or organisations who pose the threat haven't changed and are commonly seen to be:

- Nation states and not always those who appear to be unfriendly
- Terrorist groups
- Organised criminal gangs
- Protest groups
- Competitors
- Staff and contractors

The threat they pose does vary, not only with who they are targeting, but the objectives that they might have, the geographic region that any attacks take place in and how over a period of time their tactics, objectives and capabilities change. The security measures that a business adopts should reflect a risk assessment process, but the measures adopted will clearly vary between an extractive industry working in the Middle East and a financial institution on Wall Street. Operationally dealing with a physical threat from terrorism, as seen during the attack on the Algerian Amenas gas facility in January 2013, requires a completely different response to the Carbanak cyber gang, who allegedly stole USD1bn from banks across a number of countries.

Although these two examples are perhaps at the extreme, the protective methods used by physical and cyber security are fundamentally different. There is potentially a reliance on the other and one of the reasons given for convergence, is the fact that traditional electronic physical security equipment is becoming digital and sitting on an IP network. The common purpose that this equipment has in protecting facilities, the increasing use that is made of IP networks for equipment to communicate over, as well as the manipulation of data to extract monitoring information on security trends, is seen as a motivating factor. This aim is however a downstream process that should have resulted from upstream analysis, which is designed to understand the risk that a business is carrying. As operationally physical and cyber security are not the same, it is perhaps at the upstream process, where the risk to a business is assessed that any merger should take place.



The threat can manifest itself in a number of ways, exploiting vulnerabilities in protective measures as well as organisational structures

Operationally, Cyber and Physical Security Don't Mix

It is perhaps unsurprising that at an operational level Cyber and Physical security don't mix. The threat actors might be the same but the tactics used to overcome defensive measures are not. The physical reconnaissance of a potential target is completely different from sniffing out unprotected endpoints. Climbing over or cutting through a perimeter fence is not the same as exploiting the weaknesses in a firewall and being able to manipulate mechanical locks has no relation to exploiting a USB port. The ongoing daily operational response, whether it's the employment of security guards or cyber specialists will result in different tactics being employed. Even if those tactics are being directed centrally, for those on the ground there is little potential for convergence.

It is perhaps telling that advice produced by the UK government for businesses, at an operational level, on how to deal with the potential of cyber threats does not mention physical security. The measures all relate to logical controls, but whether this is a sign from those producing the advice that physical and cyber security don't mix, or whether its written from a basic perspective is not known, but it is telling.

But where there is crossover is through people and their willingness or ignorance in providing a "key" to overriding Physical and Cyber protective measures. But who owns this threat, is it Physical Security, Cyber Security, Human Resources, or the departments people work in. It is the exploitation of this or any other point where there isn't clear delineation of responsibility, which provides a weakness in overall protection.

Responsibility needs to be defined at all levels and delegated to those who have the experience, understanding and range to counter the threat.

Threat evaluation

To understand the intention and capability of threat actors, it is necessary to gather information and to undertake analysis of that information, to provide a threat picture. It is through this process, which systematically exploits open and closed sources, and takes into account leading indicators from Internal Audit reports, staff disciplinary issues, the accounts of internal and external fraud investigations, when combined with compliance monitoring that a comprehensive picture of the threat landscape is produced.

Those posing the threat provide not only straight line attacks, either physical or cyber but can blend these. If reports of the Carbanak attack are correct, it has been suggested that internal CCTV cameras were used to capture the actions of bank staff. Whether that occurred or not is unknown, but the potential for security systems to be exploited has been recognised by the UK's Centre for the Protection of National Infrastructure, (CPNI), through a guidance document, *Physical Security over Information Technology.* It is perhaps at the level of threat assessment, understanding how a threat presents itself and how it can exploit physical and cyber vulnerabilities that any merger between the two disciplines should take place. The production by analysts of threat assessment documents should lead the way in allowing vulnerability assessments to be made, impacts measured and the security risk evaluated.

Although it might be the case that a single document marked "Security Risk Assessment" is produced, it is highly likely that it is constructed over several layers. Each layer is in effect an individual risk assessment and in the case of physical security this could be to do with the risk of overseas travel, Tiger Kidnapping or the protection of business Critical Infrastructure. It is by taking each of these individual reports and treating them as a product for inclusion within other risk assessments that a true picture of the risks posed across a range of issues could be generated.

Operationally, Cyber and Physical Security won't merge but the risk has to be understood and responsibility delegated to ensure there are no gaps

So will Cyber and Physical Security Merge

At an operational level, it is very difficult to see how the two disciplines could merge. The method in which vulnerabilities are identified and overcome is different. There is however a common threat and while the threat will act in different ways, there needs to be a rounded understanding of the challenges posed. This could be achieved through a centralised collation and evaluation system that examines common threads, blended attacks and provides a picture that realistically measures the threat as it presents itself.

Merging any function requires a depth of thought and a clear understanding of what the expected outcome would be. Physical and Cyber security might be working towards the same goal, protection of an organisations assets, but the methods in which this is achieved are not the same and it might be to the detriment of both if this were to occur.

The Risk Management process is a method by which all risks to an organisation are recognised and treated within individual risk appetites. By ensuring a free flow of information, across an organisation and not just between Physical and Cyber Security, will allow risk reports, prepared by those with the relevant competence, to be included within other reports where the information would be of benefit.

But primarily perhaps, there has to be a clear delineation of responsibilities to ensure that there are no gaps in the protective measures. This goal would be achieved through the merging of Physical and Cyber Security Policies but perhaps not the two disciplines.

RedLeaf Consultancy provides services to enable clients to manage their security risks. For more information visit: www.redleafconsultancy.co.uk

Or to discuss your needs email: info@redleafconsultancy.co.uk