// Physical Security

Security strategies come from a place of knowledge and awareness and include multiple vectors of exploit from across the "Digital, Physical and Human".

About Cyberfort

Cyberfort exists to provide our clients with the peace-of-mind about the security of their data and the compliance of their business, which is much needed in our increasingly data hungry world.

Since we were established in 2017, we have brought together technology, people, expertise, facilities and leaders in cybersecurity to create a capability that is second to none. Our vision is to create a safer world for us all to live, by creating safer organisations. To do this we want to be recognised and trusted for our excellence in everything we do. We aim to be an authentic leader, with a human voice in a world that is increasingly digitised and robotic.

While many focus on the digital elements of cybersecurity to protect assets from incorporated threats, they leave the vulnerabilities from Physical and Human exploits to go unidentified until exploited.

It would not be unusual for the Physical and Human elements to be no more than tick box exercises. Performing internal risk assessments and awareness training as part of a team members induction and updated periodically or as a result of an incident.

Actors will exploit this thinking and take advantage of these gaps, as things get over looked. It can also be easier to hack a human rather than a system whilst leaving less of a forensic footprint.

Many people will assume that they are too small or security is irrelevant to their services, unfortunately this is rarely the case, they might not even be aware that they are in a supply chain or holding critical personal information for a person of interest.

The Physical Security and Social Engineering services we provide are designed to identify vulnerabilities in both Physical and Human methodologies deployed. This then allows you to address these gaps through controlled manors, rather than as a result of being exploited.

In order to gain access or control your assets we deploy simulated penetration testing exploits. These simulations are designed and carefully planned to identify both internal and external weakness which could be exploited by hostile parties for personal gain, criminal or malicious reasons.

Deploying trained specialists with a unique set of skills provides you with the knowledge of vulnerabilities identified during the process and recommended measures to implement in order to reduce or limit exposure, improve response and reduce risk.

Cyberforts services encompass 5 separate activities:

Invited Assessments

An audit style review of your facilities or assets. We'll look at your processes, policies, methodologies and counter measures in place. From this we gauge the culture, base levels of training and awareness across a business. The key outcome from this service is to identify key vulnerabilities without testing and raise awareness.

Full Health Check

A full health check will require an in depth scoping workshop, as this is a bespoke engagement that is aligned to your market vertical, specific facilities and rules of engagement. We will use a mix of methodologies to attempt engineer a desired outcome via legitimate and illegitimate methods. This would be used to simulate both criminal and state actors methodologies. The outcome of this will be identification and testing of vulnerabilities with little or no prior knowledge, gaining an understanding of culture and base-levels of training.

Lite Health Check

A great analogy for this service is a Pro's version of playing knock down ginger, also known as Buzzing a target. We light test your perimeters and reception or public access areas. This is to gauge weakness against opportunistic criminal elements, over targeted attacks or state actors. We recommend the full health check first and then to have a lite test every 6 – 12 months.

The Challenge

This bespoke service engagement is utilised for testing a specific process or protection for an asset. Through the use of methodologies we attempt to engineer a single desired outcome via legitimate and illegimate methods. Desired outcomes could be placing an item in a secure area, removal of a dummy item or breaching a specific room. The outcome of the The Challenge would be to test security measures protecting a specific asset.

Remote Exploitation

This service focuses on the people within the organisation and the ability to gain information from an external attack vector. Using a number of methodologies we will perform social engineering tactics to build pictures of what information can be gathered or requests carried out. This would be used to simulate both criminal and state actors methodologies.

Due Diligence

When purchasing a business or selecting a vendor you would need to carry out technical, cyber and many other due diligences. Our service ensures that the front door is not propped open. This package combines health checks, remote exploit and an initial assessment to gauge weakness against opportunistic criminal elements, organised crime and state actors that produce risk factors.

Key Features and Benefits

- Establish vulnerabilities and highlight how these may be exploited by hostile parties internal or external for personal gain, criminal or malicious reasons.
- These tests identify physical weakness and help build a security culture within the organisation but also assist in appropriately assessing measures.
- Uniquely scoped to each clients requirements.
- Using deception techniques to manipulate individuals or groups into divulging confidential or personal information in order to perform fraudulent actions or gain access to assets.
- These tests identify human weakness and build a security culture within the organisation by allowing the situation to be appropriately assessed.
- Combined with physical and/or technology assets can be uniquely scoped to each clients requirements.
- Training staff to be aware of threats posed by social engineering looking at the types of attacks utilised by both criminality and government agencies.
- Particular attention paid to the risks associated with social media.
- Operating methods and physical security philosophies.
- Customer elements can be defined through scoping for example counter surveillance techniques or physical protection methods.

How we have helped one of our clients

A prominent global supplier of Oil and Gas product and services was involved in the process of hydraulic fracturing. A procedure that had faced considerable opposition and negative publicity throughout the UK. As such there were concerns for the safety of staff, specifically from activists who had previously conducted direct actions in the form of lock ons / office invasions etc. There was also concern relating to state actors and industrial espionage.

We were contacted and asked to conduct a social engineering piece against staff at the London HQ, with the objective of accessing the building and retrieving commercially sensitive material.

The Solution

We deployed a four person team in the vicinity of the customers London HQ, for a period of 5 days, to initiate an intelligence gathering evolution, culminating in a series of social engineering probes to discover the porosity level of their customers security.

Results and Benefits

An operative was able to access the building and the offices, bypassing the existing security measures both physical and human, and gain imagery of highly sensitive thermal data relating to oil deposits within the UK.

As a result of this action staff received training and familiarisation of social engineering techniques as well as awareness training of specific threats relating to their business.

Consequently a security culture was developed amongst staff, and physical measures ere enhanced, further protecting the customers global interests.