RedLeaf Consultancy
A Security Practice

Six Ways To Lose Information

Every so often the compromise of sensitive information makes the news headlines, whether it's the discovery of UK Ministry of Defence, "Top Secret" documents at a bus stop or the theft of a pharmaceutical company's research by a foreign state. Although infrequent, these incidents are only likely to be the tip of an iceberg that has not been explored, as information loss is rarely known about and in itself, difficult to prove.

Even though it might be difficult to prove and probably embarrassing if a document left lying on a desk is stolen or a conversation in a café overheard, in themselves single incidents might not have a detrimental effect. It is the cumulative and systematic exploitation of a range of sources across a period of time and by a variety of means that can cause serious damage. Set out in this paper are 6 ways in which information can be lost, none of which involve cyber theft, there is no need!






1 There Is Nothing Confidential About Confidential Waste

Walk into just about any office anywhere and dotted around the floors and in print rooms will be bags or bins for the disposal of confidential waste. But in itself the term, "confidential waste", is a misnomer as it gives the impression that sensitive material, from the moment it is dropped into a bag until the moment it is shredded is secure, which it isn't. At any point along that process, it is open to theft and while most of the material might be innocuous some of it won't be, particularly if departments, known to be working on sensitive information, are targeted. Who is going to notice if documents are removed, put into a general waste bag or briefcase and taken out? The answer is probably no one.

2 Open-Source Intelligence – It's Everywhere

The use of the term "intelligence" probably conjures up images of secretive government agencies and certainly they use Open-Source material in their intelligence operations. However, all that Open-Source means is that it is information, in whatever format, which is publicly available and ranges from company accounts to conference presentations. Although the impression might be given that any search is limited to Google, in reality, as with government intelligence agencies, this is the systematic exploitation of a wide range of source material on the targeted organisation or individual concerned. It might be the case that separate pieces of information do not matter, but it is the collective view of all that information, combined with its analysis, which can provide a clear picture of an organisation's secrets.

3 There is no Secret in Open Plan Offices

Open plan offices, with their rows of desks and computer screens together with centralised print facilities, provide an ongoing opportunity to overhear and oversee information. Although there is some degree of territoriality, in that people tend to sit at the same desks with same people each day, the opportunity to appropriate information is wide, with information being left on desks and conversations overheard.

This is a problem that has been compounded both by the use of hot desking and flexible working. The territoriality that existed in open plan offices is no longer there and the feeling of owning a space is lost. There is no indication of who neighbours are, which apart from the potential for direct information loss could lead to a laissez-faire attitude to security and reduce the overall effectiveness of the measures that there are in place.

4

Working from Home

Although some employees always worked from home, Covid-19 has driven the practice with an increasing number of companies telling their staff either that they only have to come into the office on a few days of the week or in some cases, not at all. The problems with home working are now well known, with the potential that there is for the compromise of information to take place, but it is the longer-term issues, which are of more concern.

The triggers that there are in why people compromise information, whether it's an unresolved grievance, associations with hostile 3rd parties that go unnoticed or the exploitation of loneliness, which could lead to increased risk. On top of that, even simple things such as the separation of household waste into different bins for recycling, makes it easier (and cleaner) for anyone searching for documents that have been thrown away.

5

People Making Themselves Targets

People like to talk and some people do it more than others, their conversations can be overheard as they speak louder than anyone else in a café or on the train, their LinkedIn profiles seem to contain every facet of their work and maybe unwittingly they draw attention to themselves.

It is the classic example of how potential sources are recruited, whether it is the person who is at the centre of the information, the security officer who is there to protect it or the cleaner who tidies up after them.

6

Threat Awareness – Or the Lack of It

Perhaps one of the greatest threats in the protection of information is a lack of threat awareness, from the most junior member of staff to the most senior of executives. Rifling through confidential waste, searching the internet and deliberately listening to people might seem like something without basis and as a result effective measures are not put in place or enforced.

There can be the assumption that the information an organisation has isn't valuable and the incorrect belief that just because they display high moral standards others will as well. However, it is this attitude which is an enabler for anyone who wants to steal information.

RedLeaf Consultancy
A Security Practice

The protection of information is a risk issue for the organisations concerned, it is after all only they who understand what any compromise might mean for them. However, there has to be an understanding of the Threat, including who the Threat Actors might be, the tactics which could be used and this has to be brought within the Risk Assessment, along with the control measures that have to put in place and captured in the governance regime.

Threat Actors, together with their abilities, will vary and not all of them will be sophisticated nation states, as their individual information requirements will be different. The needs of a protest group are maybe not the same as a member of staff, whose needs are maybe different from that of a journalist, but each must be addressed within a Threat Assessment.

The intention of this document is only to outline 6 of the ways in which information can be lost, there are others, all of which have the intention of providing a constant supply of material, rather than just snippets of it. For a greater understanding of the issues involved in the protection of sensitive information contact RedLeaf Consultancy.

To contact RedLeaf Consultancy:

Email: info@redleafconsultancy.co.uk

Visit: www.redleafconsultancy.co.uk