# Is your business oblivious to icebergs?

H20; one of the staples of life and one of the most abundant resources on the planet, filling the vast expanses and deep chasms that separate the continents. The sea captures our hearts with its timeless beauty and serenity whilst being home to a plethora of mammals, birds, reptiles, amphibians, fish and various other aquatic species. Crossing it, was the pride of the great steam ships of the 19th and 20th centuries.

Dominated by air travel now, ships and the sea once formed a symbiotic relationship. A ship wouldn't exist without the sea, and traveling across the sea was not possible without ships; quite the conundrum. But drop the temperature of the sea to below freezing point and now we have a real conundrum. Suddenly the sea is fraught with peril as icebergs form. A simple physical change of state from water to ice turns the essential element that allows a ship to be of use into its greatest enemy.

Let's compare this with a similar scenario in information security. Your business relies on humans. Without humans it could not function. True, technology affords us autonomy, but that technology is still designed by humans and serviced by humans, should it fail, making humans an indispensable asset to your business. But then change the state of a human from the loyal, diligent hard working employee who seeks gratification in what they do into a greedy, self-indulgent individual who sees the value in what your business offers and wants to leverage it for their own gains; and you have just changed your greatest asset into your biggest peril.

Just as the lookout, colloquially known as the crow’s nest, was used by a ship's crew to detect icebergs as far in advance as possible, you need to be on the lookout for early warning signs of employees that could develop into icebergs whilst your business is steaming full speed ahead.

The first iceberg to look out for is the disgruntled employee or disgruntled former employee. Early signs may be visible when employees start acting suspiciously or displaying abrasive behaviour shortly after being passed over for a promotion; demoted; excluded from a project; included in a project of no interest; denied the chance to contribute ideas or being terminated for a multitude of reasons. The real danger arises from the intimate knowledge an employee or ex-employee has of the weaknesses that your business exhibits.

The second iceberg is contractors who are often given similar access privileges to employees in order to conduct their work. Whilst most contractors will not have any malicious intent; due to the limited contact with contractors it is much more difficult to gauge trustworthiness and fewer reasons for contractors to have any sense of loyalty to your business, considering you are not their employer. It is therefore, critical to closely monitor the behaviour and activity of contractors.

The third iceberg is the new employee. Just like the contractor, your working relationship with new employees is limited and you are assuming a level of trust that has not yet been verified. To add further complications, new employees are less likely to be familiar with policies and procedures resulting in simple mistakes that could have huge implications on security. Peers and managers should closely monitor new employees.

The fourth iceberg to watch out for is the employee with privileged access. Maintenance, security and janitorial staff are all examples of personnel whom have been granted a high degree of physical access. A janitor, often needs access to every room in a building in order to clean it, but suppose the janitor decided to install a keylogger; power down a critical piece of technology; or start piecing together a shredded printout of credit card details. Surveillance systems and correlation of incidents with physical access to otherwise highly secure areas of a building are essential to provide clear evidence of wrong doing by personnel whom have been trusted with privileged access in order to carry out their jobs.

The fifth iceberg, and one that is often overlooked is the well liked, friendly individual who is always cheerful and will bend over backwards to be of assistance. This type of employee usually likes to avoid conflict and will easily comply with requests for assistance without giving much thought to the authenticity of requests and the possibility that someone could use authority to elicit help for evil purposes. The accidental insider, though not malicious, naively, and innocently aides and abets criminal activity. HR and managers should identify people that fit this description and provide additional training about the dangers of social engineering and the need to establish authenticity of a request before complying. It will often go against their nature; but with the correct level of coaching this threat can be significantly reduced.

In the same way a change of state from water to ice can spell disaster for ships at sea, a change in state of your employees can turn your greatest asset into your biggest peril. You can charge full steam ahead oblivious to the warning signs or you can choose to be on the lookout for icebergs among your employee base.