KCS Group Europe

Cyber Wellbeing: a corporate necessity?

29th January 2021

Back in 2015, a disgruntled employee of the supermarket group Morrisons was given an eight-year sentence for leaking the payroll data of roughly 100,000 employees online and to newspapers. It was ruled that Andrew Skelton clearly had an axe to grind with Morrisons when he leaked the sensitive data of those 100,000 employees. Five years later, it was determined by the Supreme Court that Morrisons was not liable for the damage caused by the leak.

The ruling set the precedent that a company does not have to be responsible for the cyber welfare of their employees, but is that right? Does there need to be a change in the attitude that businesses have towards cyber-security?

Whether one is dealing with a government intelligence agency or a private business, insider threats should be taken just as seriously as outside ones. Taking the Cold War for example, infamous cases like Aldrich Ames, Oleg Gordievsky and the Cambridge Five demonstrate how damaging insider threats can be. In these cases, the 'bad actors' were able to operate for so long due to a direct lack of competency by the agencies in question in identifying and plugging gaps in security. Private corporations now need to have that same responsibility regarding cyber-security: nothing short of total oversight on what data is held, who can access it, and the ways in which it could be used nefariously will do.

The Morrisons case has set a concerning precedent. Morrisons was not found liable for the data leak because the compromise was intended to hurt the company itself. However, it is very likely that practically data breaches within a company disadvantage the company in some shape or form, particularly in the reputational area. So, whenever a data leak happens the company would not be found liable. The effect of these current laws diminishes the responsibility of the employers regarding the protection of their employees in the event of a data breach caused by an insider. Even though the data breach in question did not benefit the company,

KCS Group Europe

Cyber Wellbeing: a corporate necessity?

Morrisons was and still is responsible as the creators of the conditions in the business and cyber environment that allowed Andrew Skelton to release the sensitive data of 100,000 employees. Businesses must take responsibility, as much for the safety of their employees as for the general sake of the business itself, especially when it comes to insider threats. While these cannot always be predicted, they must always be countered where possible, and mitigated where not.

What this ruling shows is that cyber security needs to be taken very seriously and that all business are at risk of suffering from a data leak from which the employees may not legally be entitled to some form of compensation. It also means that services like cyber-insurance and consultancy have become a necessity to ensure that the employees do not become the overall losers of a data leak.

There needs to be a change in attitude from the top regarding cyber responsibility. While the laws that make employers responsible for the physical and mental wellbeing of their workers are important and necessary, there needs to be the same level responsibility enforced regarding the cyber wellbeing of the same. Seeing as cyber-attacks, whether inside or outside threats, can be extremely damaging to a company and its employees, cyber welfare must extend to doing everything possible to prevent a breach, and subsequent mitigation and compensation should this not be doable. Otherwise, trust in a firm may irreparably break down from within and without. That this may necessitate a change in the law, should not be a barrier to right action being taken and further reinforces the idea that pro-activity should be a constant watchword to look at the threat picture differently and understand the true range of risks posed through cyber.

.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening.

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

To find out more or to arrange a meeting to discuss your business needs, please…
email the team at info@kcsgroup.com or call (00 44) 2072451191