Coronavirus - Information Risk Assessments

As businesses plan their return to their offices following the COVID-19 pandemic, there are a myriad of issues to consider but unlikely to be high on that list is the risk of a data breach or cyber-attack.

For most organisations, the return to office working will be a more gradual process than the sudden move to homeworking at the start of the lockdown and this 'hybrid' working could pose significant additional risks to the business.

Added to this, it is now widely accepted that people are the weakest link in the information security chain, with almost 90% of all data breaches and cyber-attacks being caused by employees or significantly contributed to by them. It is often just one mistake by an employee who opens the wrong email or clicks on the wrong link, particularly when they think that email comes from someone they know, that spells disaster for the business.

Undertaking an information risk assessment, required by GDPR Article 35, will enable you to identify and prioritise information security risks and implement appropriate security controls (required by GDPR Article 24) to avoid that disaster.

Information Security is about maintaining the confidentiality, integrity, and availability (CIA) of information. If any of the elements of CIA are compromised, a GDPR breach has occurred.

Undertaking an information risk assessment can be relatively straightforward, involving the three steps of risk identification, risk analysis and risk evaluation.

1. Risk Identification

Risk identification involves identifying the threats such as the internal and external events or causes that would have adverse consequences, and vulnerabilities - namely weakness in the information security system - that pose the risk.

2. Risk Analysis

Risk analysis is the combination of the likelihood of that event or cause and the consequences of the identified risk, should it occur. As with health and safety, a 3 x 3 or 5 x 5 risk matrix can be used to quantify the risks.

3. Risk Evaluation

Risk evaluation involves comparing the risk scores to determine if the risk is trivial, acceptable or unacceptable, and implementing controls accordingly.

A relatively small amount of time undertaking information security risk assessments during the planning of the return to office working, particularly during that 'hybrid' period, could both avoid a serious breach and ensure compliance with GDPR Article 35 and 24 duties.

Written by:

David Sinclair, Senior Solicitor at rradar

Dislclaimer:

This article has been provided as an informational resource for rradar clients and business partners. It is intended to provide general information only to employers in the current exceptional circumstances arising as a consequence of the Covid-19 pandemic and is not intended to provide legal, taxation or commercial advice or address legal taxation or commercial concerns or specific risk circumstances of any particular individual or entity which should not be relied upon. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Due to the dynamic nature of infectious diseases, circumstances may change and rradar cannot be held liable for the guidance provided. We strongly encourage readers to seek additional medical information from sources such as the World Health Organisation, Public Health England and NHS.