ALTERNATIVE
SOLUTIONS

Why Do You Need an Information Security Officer?

Introduction

Businesses rely heavily on their data. It enables them to carry out their day to day tasks and help increase revenue. This data can be electronic or held in filing cabinets as hard copy. An organisation's data is important and how it is protected is vital for survival. The protection of the data can be technical but this is not sufficient to prevent data breaches, because vulnerabilities in software and hardware are discovered every day, making it more difficult to ensure the data is protected at all times. Combining technical protection with non-technical controls, such as security education, policies and procedures can give the layers of protection needed to ensure data is not compromised.

How Would an Information Security Officer Help?

Information Security Officers (ISOs) establish and enforce security policies and procedures to protect an organisation's computer infrastructure, networks and data. ISOs play a vital role in protecting the organisation and its reputation by helping to prevent a data breach which can result in business disruption, loss of confidential or commercially sensitive data which can lead to a financial loss.

ISOs take responsibility for educating employees about their information security responsibilities by highlighting the existence of policies and procedures. Traditionally new employees are given copies of security policies (if they exist) and told to read them during their induction process. With the pressure of starting a new job it is unlikely the policies will be fully understood or adhered to. To enforce the policies, an ISO relates them to real life which makes them a lot easier to understand. They will also provide ongoing training to ensure employees are up to date. By explaining and discussing the documents with employees, the ISO is visible and approachable, allowing employees to ask questions or raise concerns.

An ISO is also responsible for incident management, reporting the impact on day to day business and advising on possible controls to prevent a similar incident happening again. By maintaining incident management reporting, patterns can emerge where the same incident is being reported repeatedly, indicating training is required. This increases further the security of data.

Having a single person accountable for information security, which more importantly the organisation knows is responsible for information security, provides a high level of assurance for clients, partners and regulators that you are properly managing and controlling information security.

Alternative Solutions Limited
PO Box 176, Cirrus House
Garenne Park, Rue de la Cache
St Sampson, Guernsey, GY1 3LQ

T: 01481 701234 **F:** 01481 715718
W: www.asl.gg **E:** info@asl.gg

Registered in Guernsey 16421

ALTERNATIVE
SOLUTIONS

About the Author

Sonia Bowditch is a fully qualified Information Security Officer with over 17 years' experience working in the Finance industry. She holds an MSc Information Security from London University and has qualified as a Certified Information System Security Professional (CISSP). Sonia can be contacted on 01481 701234 or by emailing sonia@asl.gg.

Alternative Solutions Limited
PO Box 176, Cirrus House
Garenne Park, Rue de la Cache
St Sampson, Guernsey, GY1 3LQ

T: 01481 701234 **F:** 01481 715718
W: www.asl.gg **E:** info@asl.gg