PROTECTIVE
INTELLIGENCE

CASE STUDY
PROTECTION STRATEGIES

CASE STUDY
PROTECTION STRATEGIES

A Serious Problem

A recent survey by the Department for Business Innovation & Skills revealed that;

— Of all the security breaches considered to be 'most serious' by UK businesses, a staggering 51% were caused by staff either inadvertently or deliberately exposing information.

— The average cost of a 'most serious' breach was almost £1m for large organisations, and nearly £100k for small organisations.

— Almost 40% of all organisations do not provide any on-going security awareness training to their staff.

— 70% of companies where security policies were poorly understood had staff-related breaches.

It's somewhat of a cliché to say that the employees are the greatest asset of any organisation, but it's absolutely true that they can also be its worst enemy.

Our Approach

New Thinking on Information Security

Information Security needs to change. For too long, the protection of information has taken a backseat as technology drives the security agenda. We believe that the challenge is to move information security into the heart of the organisation, where everyone understands the importance of protecting data from loss, corruption or exposure.

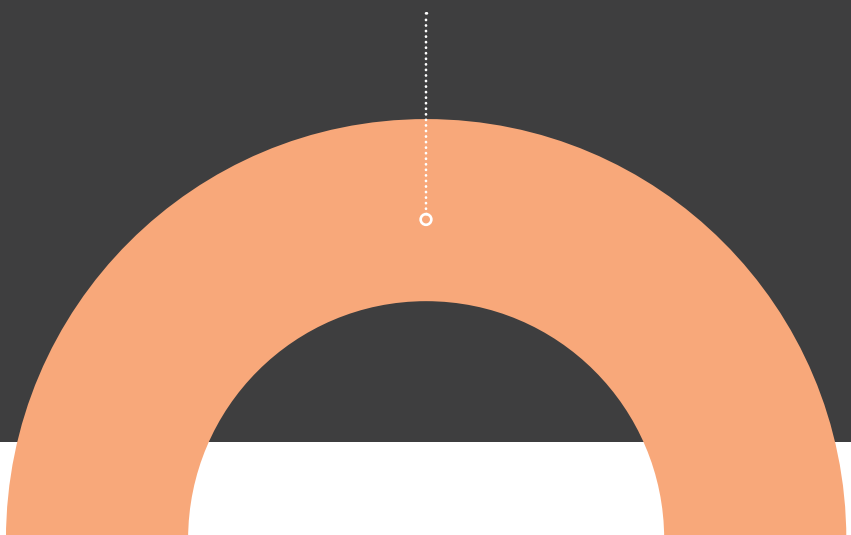
Information Protection is Unique

We have vast experience in delivering effective Information Security & Protection strategies into organisations of all sizes. Whether you are creating a strategy from scratch, or you need to review and update your existing policies, we can help.

We don't provide you with a standard 'off the shelf' strategy, we take the time to understand how you operate. We investigate what threats and vulnerabilities you face, and balance this against the realities of how you need to work.

51%

OF UK BUSINESS' 'MOST SERIOUS' SECURITY BREACHES WERE CAUSED BY STAFF EITHER INADVERTENTLY OR DELIBERATELY EXPOSING INFORMATION.



CASE STUDY
PROTECTION STRATEGIES

The Case Study

A very large, global business engaged us with a view to creating a new Information Security Strategy after suffering from a number of security breaches which incurred significant losses – one of which was valued at over £20m. After reviewing their current Strategy and Policies, we discovered four key areas that needed improvement;

- Their current strategy was too focused on technology, with little attention given to the human factors in Information Protection. The result was a strategy that dictated technical solutions ("You must use this specific type of Firewall") but neglected to consider the wider implications of security.
- Information Security decisions were based entirely upon what the IT Department thought it should be doing, with no input from the business.
- There was no clearly identifiable single point of contact for the business to engage with for Information Security concerns.
- The current practices of the IT Department were directly contributing to the loss of information, with issues such as cloning current or former user accounts for new starters, failing to revoke access for users who had moved on, and neglecting to fully wipe desktops, laptops and external hard drives prior to re-use or disposal.

After discussing the results of our investigation, we agreed to revise their Information Protection Strategy to bring them in-line with current standards, and to give them the flexibility to continue working in a secure fashion without being over-burdened with security. Central to the new approach was the creation of an Information Security function within the business, reporting directly into the Chief Information Officer.

This enabled the security function to have a voice at C-Level, gave the employees a single point of contact for information security issues and advice, and allowed a clear demarcation between information protection policy and security technology.

Other improvements included;

- A significant reduction in security breaches.
- Installation of a risk-based information protection
- approach to ensure appropriate protection levels.
- Established a regular, on-going Information Protection Awareness programme for staff, which provided baseline training for everyone and specialised courses for those who needed more in-depth training.
- Enabled a programme of regular monitoring of Information Security Awareness, enabling management to analyse metrics on how well the company was performing.
- Revamped processes within the IT Dept. to eliminate processes detrimental to security.
- Enhancing the in-house Project Management function by including Information Security in the appropriate checkpoints and gates, helping to ensure that no applications were released onto the estate without first being security accredited.
- An increased level of Information Protection awareness amongst staff.
- Prove that all information assets were being appropriately protected and monitored.
- Establish a positive Return on Investment, when the Information Protection budget was compared against previous losses.

THE CORNER HOUSE
24 NORRIS ROAD
UPPER ARNCOTT
BICESTER
OXFORDSHIRE
OX25 1NZ

+44 (0)1869 247814
info@protectiveintelligence.co.uk

protectiveintelligence.co.uk