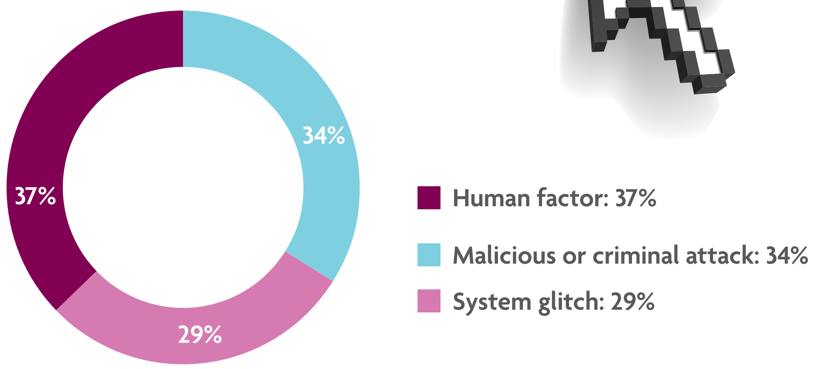
Plugging the **information leaks** in your organisation...

Businesses are becoming increasingly dependent on digital technology to operate. Consequently, the changing digital workplace has resulted in greater amounts of sensitive company data being placed on physical storage devices, housed in the cloud and on servers, and made accessible through social networks, intranets and on smart phones/tablets. While of course this brings clear advantages, it also means organisations are increasingly vulnerable to system failures, data losses and cyber attacks.

It's therefore of no great surprise that for the sixth consecutive year, the cost of lost or stolen information has continued to rise, with the average organisational cost to a business suffering a data breach now **£2.04m** (2012), up from £1.75m in the previous year. Costs incurred include: repair costs, operational shutdowns, loss of business, investigative and notification costs, legal expenditure, and **REPUTATION DAMAGE**.

Businesses are of course, trying to address the rising problem. Last year alone, worldwide organisations spent **$114 billion** trying to stem the data breach tide, with many businesses investing entirely in security technology. Yet employee negligence continues to be the most common cause of data loss.

Most common cause of data loss:
EMPLOYEE NEGLIGENCE



Examples of employee behaviour putting company information at risk includes:

- ✗ Using weak and unsafe passwords
- ✗ Opening suspicious emails or attachments
- ✗ Leaving laptops / smartphones unguarded
- ✗ Publishing unapproved information on social networks
- ✗ Storing unencrypted information on memory sticks

There's no doubt, technological infrastructure is crucial in reducing data breaches. But correct employee behaviour is the foundation to the success of the technological investment. And with the continued explosive growth in digital information, plus improvements to mobile and connected technology fuelling the trend towards a 'virtual' workforce - Company information will be placed at an even greater risk.

Clearly, to reduce information breaches, it's crucial organisations build a security-conscious corporate culture.

But how can this be achieved?

Organisations must take a strategic approach.

The following is the methodology we used to help change employee behaviour at the worlds 5th largest organisation.

Research

Firstly, undertake in-depth research (surveys, focus groups etc.) to identify the types of employee behaviour that is placing company information at risk and the reasons as to why employees are undertaking the behaviours.

Surveys should then be routinely carried out to help inform the behaviours that require greater attention. Surveys must also act as benchmarks, against which future behaviour change can be measured.

Raise awareness.

The goal here is to make employees aware of the threats data breaches pose. These communications ideally need to be 'shocking' and focus on the consequences of incorrect behaviour for both the organisation and the employee.

Real life examples/scenarios are particularly effective, especially when tailored to the environment the employees operate in.

Video proved to be a very successful medium to employ.

Educate employees.

Toolkits (based on the behaviours identified in the initial research) should be supplied to leaders, so that they are equipped with the right information to educate employees.

It's important that once the information has cascaded down from the leaders, it is further spread through the organisation by employees, who become 'sharers' or 'champions'. They help facilitate two way dialogue, creating bottom up communications.

Given that IRM is a dry subject area and one that is somewhat shrouded in mystery to the employee, it's imperative that an open dialogue is encouraged using dynamic language, in order to make the topic more interesting, clear and engaging.

Training.

New behaviour has to be practiced in order to be adopted. And spotting information risks is a skill that improves greatly with experience. However, due to the nature of IRM, it's not something you can easily practice in the real world.

We created a suite of digital games that allowed us to replicate real world situations in a virtual environment. The games provided interaction with the campaign messages, meaning the behaviour demonstrated in the gameplay was likely to be transferred to real life situations. The games also added more excitement, making the dry topic more appealing, and changing the way IRM was discussed.

You can find a more detailed case study on the games, here.

It's important that communications have an interactive element, which require the employee to make a decision. This is because IRM simply boils down to the employee either making the right or wrong choice.

Risk management processes.

Of course, humans make errors. So it will never be possible for an organisation to completely eradicate data leaks. Given this, as well as training employees on how to spot and stop data leaks, employees must be trained on how to respond when a data leak occurs.

Creating a set of business processes for employees to follow in the event of a data leak is crucial. Often, by following the correct processes employees can significantly reduce (if not eliminate) the threat a data leak holds.

Conclusion

Creating a security-conscious corporate culture is not something that can be achieved after a single internal communications campaign. Culture has to be continually cultivated. It is therefore important that employees are constantly engaged with IRM, so that the behaviour becomes second nature.

The costs of potential data leaks far outweigh the costs involved in achieving a security-conscious culture.

Contact us

For further information or assistance on changing the behaviour of your organisations employees, contact us.
info@rimadesign.com

References:
PWC. Cybercrime: protecting against the growing threat. Global Economic Crime Survey.
Symantec. 2013 Cost of Data Breach Study: Global Analysis.
Lloyd's 360 Risk Insight: Managing digital risk Trends, issues and implications for business.
UWCISA. Information Leakage & Data Loss Prevention.