Why creating a culture of data security is essential

Posted on 23rd February 2017

All businesses collect and hold personal data about their customers, employees and other individuals that they have dealings with. This data is a valuable asset and businesses are (rightly) investing resources to protect that data by putting in place technical and organisational security measures.

But these measures won't work, (or at least won't work as well as they should), unless those tasked with putting them into effect – employees – understand and accept the need to comply with those measures. The best way to ensure that happens is to create a 'security culture'.

A good security culture is both a mindset and mode of operation that's integrated into day-to-day thinking and decision-making.

THE CAUSES OF POOR SECURITY

Most security breaches are caused by employees. Employees may be unwilling to comply with data security measures because they don't understand the possible impact on the business of violating it. E.g. an employee might download some software, (even if they have been told not to do so), because this would not be perceived as doing something 'wrong' or potentially harmful to the business.

If employees observe others in the organisation breaking data security policies and 'getting away with it' they will be tempted to do the same: Such behaviour becomes acceptable and normal.

When employees want to get on with their job and data security gets in their way, they will be tempted to circumvent that security regardless of the degree of risk they might expose the business too.

CREATING A SECURITY CULTURE

The key aspect of achieving a security culture is to demonstrate to employees how data security policy violations can have a direct financial impact of the business (and possibly the security of their employment).

A good way of doing this is by way of a training programme. Unfortunately, many of these training programmes tend to focus on simply setting out what policies and procedures employees are required to follow-without actually explaining why they should do so. Good training also focuses on specific threat scenarios with examples of real cases to explain why data security is important.

An essential element of achieving a security culture is to have strong senior management support: Leading by example is the key to changing the perception of employees in the business. If employees see their managers taking data security seriously by following it themselves and not tolerating transgressions they will follow the example set and comply with set policies and procedure.

MOTIVATION

To effectively protect the data of a business, security measures should be developed and implemented that not only ensure compliance with legal and any regulatory requirements but also to ensure that the motivations and attitudes of employees are taken into consideration.

When data security solutions are created to fit into employees day-to-day jobs, rates of compliance increase and a positive outlook towards data security results, which will turn lead to a healthy, stronger and more objective security culture within a business.

Another good way of motivating employees to participate in a security culture is to encourage them to make suggestions for improving existing measures. This will cause them to 'part own' those measures and encourage them to comply.

CONCLUSION

The absence of a security culture will cause uncertainty and lead to data security incidents (and possibly serious data security breaches), a situation that no business should risk happening.

For any business, a security culture should be regarded as a fundamental matter to be addressed: If neglected, employees will not develop habitually secured behaviour. Employees must understand the potential risks, as well as the benefits, of compliance behaviour, both to themselves and to the organisation they work in.

Compliant behaviour comes directly from employees being interested in security and not a result of the obstacles of threats imposed upon them.