Why your business needs to take IT security seriously

This entry was posted on March 22, 2016 by Albie.

In our upcoming series, King of Servers puts the spotlight on IT security and the worrying number of businesses still failing to take the issue seriously.
OK, so your business is going from strength to strength, you have the money to invest in new and innovative technology that will boost your operations and efficiency, you're great at what you do - but how much effort are you putting in to protect your hard work? We'd hazard a guess that you aren't taking the same steps to safeguard your operations as you are to expand, improve and thrive.

Why do we think that? Well, research carried out by Spiceworks, which was published in late 2015, revealed that 51 per cent of businesses are not classing security as a top priority for their organisation in 2016. This means that more than half of businesses are putting themselves at risk of cybercrime and are fully aware they're doing so. The shocking figures also revealed some 73 per cent of businesses believe their organisation is at risk of a security disaster or incident. So why isn't security something companies take seriously?

At King of Servers, we're pretty on the ball when it comes to the latest developments in technology, and we like to think we know our customers - and the wider world of IT - incredibly well. However, even we were surprised at the statistics - so much so that we've decided to base a whole campaign around the importance of security.

Pretending there isn't a problem
A major factor holding businesses back from investing in security is quite often the fact they think it does not apply to them. Yes, you may be a small business with a relatively small turnover, but do you think that valuable data and considerable sums of money left unprotected doesn't appeal to cyber criminals? In fact, the fact you are a small business makes you an even likelier target for attacks.

In its 2015 report, Spiceworks found that 62 per cent of respondents said their company does not carry out regular security audits. The question is: why not? A lack of awareness and a degree of ignorance have been highlighted time and time again as reasons why businesses fail to treat security as a priority.

We spoke to John Michael, CEO of iStorage, who said: "The most common cause we see for data loss in businesses is inadequate security policies and minimal internal awareness about the potential risks.

"This often leads to employee negligence due to the lack of education on security processes, from opening malware, storing and transporting sensitive data on unsecured devices to not backing up."

Educating the masses

Educating members of staff about the potential dangers of lax security is one simple method that businesses could use in order to prevent attacks, as a considerable number of data leaks tend to happen internally. However, it appears a considerable proportion of companies are choosing not to take this path. So, what's the solution? One idea would be introducing harsher penalties for organisations that fall victim to data leaks as the result of inadequate security.

Cliff Moyce, Global Head of Financial Services Practice at global technology consulting firm DataArt, said: "The effect of punishments on companies is highly debated - with evidence that fines have little effect. However, the possibility of sanctions against individuals can be a stronger motivator.

"Where lax security and controls results in anti-money laundering breaches or personal loss for customers, the sanctions can be very severe, including jail or personal fines, especially when any negligence is deemed to be willful or arising from joint enterprise."

And while promising to impose sanctions on those members of staff who put their employer's data at risk is a solution many organisations have adopted, some doubt that businesses are actually willing to follow this through in order to show they mean business.

Mike Dunleavy, Head of Customer Developments & Experience at Crown Records Management, said: "Who's heard of someone losing their job because of a data breach, for instance? You would think at the very least it was the starting point for a disciplinary process; but has anyone ever seen a headline about an executive losing their job after a data breach took place on their watch?

"These details should be part of employment contracts and should be part of disciplinary processes. It should be clear to everyone in the business that data matters - and that breaches are unacceptable."

One notable point about high profile instances of cybercrime, such as the Sony hacking scandal or the TalkTalk data breach, is that the biggest motivator in favour of adopting a more serious approach to security is often the embarrassment of your brand name appearing in the press. Hitting the headlines for all the wrong reasons unsurprisingly causes a loss of customer confidence - and it is this that will truly threaten a company's future.

Will things ever improve?

As the role of technology in day-to-day business practice continues to expand, the matter of security is one that will not simply go away. The time is now for companies of all sizes to take accountability for their actions, while realising the impact that damage, theft or loss of equipment and data can have on their productivity and reputation.

Many organisations continue to bury their head in the sand in a bid to avoid discussions about how to contend with an issue they believe is too technical for them. However, security is just as much to do with personnel as it is associated with technology. The physical impact that a cyber attack will have on your business is nothing compared with the potential effects of a tarnished reputation.

Still to come in our security campaign, we will look to help you the IT professional adopt safe, no nonsense methods in order to improve security within your organisation.

Original article — http://www.kingofservers.com/news/why-your-business-needs-to-take-it-security-seriously/