The Sunday Business Post
September 28, 2014

Joined-up approach ensures a secure future for your company

Companies cannot afford to be complacent about their own security

Shaun Rooney, technical director, Integrity Solutions

If you find the scale of the problem presented by keeping your company's IT security up to date a little daunting, then you're not alone. While you might not be on the radar of committed cyber criminals, that doesn't mean there's room for complacency, according to Shaun Rooney, technical director of Integrity Solutions.

"Many Irish companies are a little overwhelmed by the scale of the security problem. They read about high-profile breaches affecting other companies, but they don't know how exposed they are or what they should be doing to shore up their defences," he said.

"Whenever one of these attacks happens, companies ask themselves, 'Could that happen to us? Are we secure?' To make it worse, they're confused by the advice they get. They're told they need this web application file or that intrusion detection system, and yes, they do need all of that stuff. But they also need to stop and take stock of what they have, where they want to go and what the challenges facing them are."

Having a clear understanding of what the company's goals and strategies are over the medium- to long-term – and how security plays into those strategies – is more important than fire-fighting to address immediate threats. Having this kind of joined-up approach to security is the most reliable way to ensure new threats don't cause future problems.

"It's important to take things back to basics," said Rooney. "It took a little while to get that across to people, but it's starting to happen now. Companies are starting to take stock of what their actual risks are, stemming from the question of what the critical assets are that they are trying to protect."

Instead of trying to protect everything, it makes more sense to identify different security goals. By doing this, the company can react properly to the changing nature of security risks, as well as deal effectively with regulatory issues that might arise in future. Similarly, new technology that isn't yet available can be slotted into the strategy as it comes on-stream.

"You need to know what's happening in order to know where you should be spending the budget you have. This is the key to getting the most value out of the equipment and infrastructure you already have," said Rooney.

This also allows you to properly place the human element in the security equation.

"People are traditionally seen as the weakest link in security, but we're trying to create a paradigm shift on that and get companies to start seeing people as the strongest link in their defence. You need to get your staff onside, helping you with security," Rooney said.

"Building an awareness of the issues security poses is a much more powerful tool than pretty much anything else."

From a market demand point of view, Integrity Solutions is seeing growing demand for certain security services. In particular, an increasing number of companies are requesting penetration testing.

"In the past this was done on an ad hoc basis or as a customer requested it, perhaps because of a third-party request," said Rooney. "But now we're seeing businesses asking for it to be done thoroughly once a year, with regular reporting throughout the year on the status of their vulnerabilities. It's mostly to do with the rise in popularity of web and mobile application penetration testing."

Meanwhile, Rooney said the payment card industry is also responsible for driving a lot of security activity.

"Regulation is one of the biggest issues for a lot of what's going on at the moment, especially in the pen testing area," he said. "On top of this, a lot of companies are outsourcing their IT needs to third parties. They might be sending databases off to printing companies, for example, but they don't know what's happening to their data after it leaves their networks.

"Keeping track of exactly where that data ends up is increasingly important. Is that third party in turn outsourcing it to a fourth party? Third-party vendor risk-management is an up-and-coming area. We tend to not think about that here enough, I think."