BIZCOMMUNITY

Communication: Five key steps for the business, IT and security leader

LONDON, UK: You need to speak the same language... Tackling the risk of security breaches in companies is being undermined by a potentially damaging breakdown in communication between the information security function, IT and the rest of the business, new joint research by PwC and (ISC)² reveals.

Instead of working together toward common goals, different parts of the business often fail to understand - or even respect - each other's roles, according to the research, which aimed to gain insights into why business leaders underestimate information security risk.

Richard Sykes, governance risk and compliance leader at PwC, said: "The security of corporate information will stand or fall by the ability of the organisation's various functions to communicate clearly and effectively with one another. It takes all teams to sustain a meaningful dialogue, so a change in mindset is needed from all sides."

Miscommunication lies in the different languages understood by the three departments, so the research concludes that there are five parallel steps that business and information security leaders should take to close the gap.

Step 1:

For the business leader: Highlight risks to the board on current and emerging threats as the context for needing world-class information security standards.

For the information security leader: Avoid using complex technical language and describe business risks and the relevant controls in straightforward business terms.

Step 2:

For the business leader: Discuss future strategic technology choices and trends at board level to assess the impact and implications.

For the information security leader: Continually scan the horizon of emerging devices and cyber threats from the perspective of the business's strategic objectives and opportunities.

Step 3:

For the business leader: Rank the organisation's business units on a scale of low to high risk. For those that are high risk, consider introducing incentives for the successful implementation of security standards.

For the information security leader: Analyse the organisation's underlying business processes from an information security perspective, and develop business cases for more relevant, cost-effective controls.

Step 4:

For the business leader: Initiate ongoing workshops with representatives from information security, the business and IT, to brainstorm the threats and opportunities and to debate solutions.

For the information security leader: Forge strong links with 'natural allies' in the business, such as legal, compliance, risk and internal audit, to align business-focused language.

Step 5:

For the business leader: Over the longer term, engage the security leader more deeply in the strategic agenda and future plans, enabling that function to plan proactively into the future rather than reacting to emerging events.

For the information security leader: Ensure that information security's relevance is understood throughout the organisation, so it is viewed as a source of business-enabling solutions rather than a barrier to doing business.

Sykes continued: "Business leaders ignore information security risk at their peril. Historically, business leaders and boards have tended to regard information security as a technology issue - as reflected by the traditional reporting channels - but this is a complete misconception and needs to change."

John Colley, CISSP, managing director, EMEA for (ISC)^2, said: "The information security function, while rising in its influence across the organisation, is hampered by the uneasy relationship with both the IT and the business areas they are tasked to support. They increasingly understand they need to become enablers and speak the language of business operations, opportunities and risk. It's time for the rest of the business to wake up and support them in their endeavours."