FIFTH STEP CASE STUDY

Incident Response

The Background

In 2015, TalkTalk, the UK based Telecoms company, suffered a major cyber-attack. The banking and personal details of many of its customers were accessed, and the board's handling of the incident received intense – and negative – press scrutiny. Reputations are lost and won at moments like these, and this fact was not lost on our client, a well-known organisation operating in the Betting and Gaming industry.

> "The board wanted to protect their customers' assets, and also ensure the company had the tools and know-how to recover quickly and confidently from a cyber-attack."

The Challenge

The Betting and Gaming industry is a major target for cyber criminals due to the quality of the personal data it holds and the high volume of financial transactions. Our client was already upgrading its information security services, and wanted to overhaul its crisis response planning. The board wanted to protect their customers' assets, and also ensure the company had the tools and know-how to recover quickly and confidently from a cyber-attack. However it did not have the expertise to devise and execute an Incident Management Plan (IMP).

Our Recommendations

Fifth Step reviewed and overhauled the client's IMP, and proposed that their Business Continuity Plan (BCP) should be brought in line with best practice while adhering to Incident Management ISOs. This required the creation and embedding of a board-driven culture of incident management.

> "Our client's customers now know that in the event of a cyber-attack, effective and timely action will be taken to restrict damage, recover control and limit universal impact."

Our Solution

Fifth Step reviewed the client's existing BCP with its Chief Risk Officer and other senior staff, and worked to create an IMP framework. This led to a simulated desk-top exercise involving the board, senior staff and other stakeholders. Lessons learned were applied and the IMP was updated – these included improvement guidelines and scripts for running subsequent exercises that adhered to the overall disaster recovery schedule.

The Outcome

Our client can now provide clear assurance that they adhere to best practice guidelines and global standards. This means they are equipped to address any incident that impacts on their business in a calm and structured manner, and as an integrated part of their normal risk management system.

The Benefits

Our client's customers now know that in the event of a cyber-attack, effective and timely action will be taken to restrict damage, recover control and limit universal impact. The client's board have the confidence and procedures to steer the company's response mechanisms, use succinct delegated plans to co-ordinate recovery, and maintain the confidence of its customers, regulators, supply chains and the industry.

The Future

Our client was aware of its obligations and responsibilities, and the threat posed by the inability to respond quickly to an incident. But the future is now secure. They have embedded robust plans and tools within their business risk management processes, and these will ensure that if an incident occurs they will be able to react in a cohesive, professional manner, and maintain customer and industry confidence.

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com