Finance & Insurance Case Study – Financial Software Provider

The Client

Our client is a provider of financial software and digital transformation services developing trading systems to support trading activities. A Managed Service offering has been introduced by the client in addition to software development with increased responsibilities to ensure ongoing availability of services. The client has a mature BCM system implemented and supported by Teed since 2015.

The Challenge

In providing a Managed Service to clients, it was paramount to have in place an effective response with minimal outage in the event of an incident. The organisation had experienced some disruptive events and recognised there was room for improvement in the communications element of the response between different parties; internally, but also to vendors, clients and other external stakeholders.

The client had a myriad of plans and supporting documents and needed to bring these together in a useable form that would prove useful as part of the client's overall response system, whilst at the same time identifying gaps or areas for improvement.

An analysis of potential threats showed the highest impact event the client could be exposed to would be issues arising from cyber security incidents. Cyber security is recognised as an increasing threat with catastrophic consequences.

It was essential everything was done to ensure the client was prepared to respond to threats by addressing a range of different scenarios that could impact on the Managed Service technology capability, for example, vendor service disruption, loss of data centre, network/equipment failure, cyber security incident.

The Solution

In the initial stages of the project, it appeared that more than one response document for the Managed Service would be appropriate particularly taking account of the different actions required to respond to a physical infrastructure event or a cyber security event. It became clear during Teed's discussions with the client that a single Managed Service Major Incident Procedure (MIP) was required. Invariably the cause of an incident is not known until in the midst of the response so an integrated document would prove more effective in dealing with any event, underpinned by appropriate response procedures for specific situations.

Teed's consultant worked with the client to produce the MIP describing defined roles and responsibilities and the response and recovery timeline; major incident communication protocols were produced in visual form clearly showing who should be speaking to whom, not just within the business itself, but importantly also within the vendor and client organisations.

The MIP includes recovery task tables broken down in a logical manner to cover incident response, DR and cyber security incident response. For clarity, relevant activities were detailed within the phases of response to a cyber security event: Detection, Analysis, Containment, Eradication, Recovery. In developing the overarching document, the consultant recognised the importance of showing how the MIP links with the organisation's other technical procedures and relevant response documents.

As with all response and recovery documents, the MIP needed to be validated to ensure its effectiveness. Exercise and awareness sessions were held involving operations teams and other relevant individuals who were taken through a number of scenarios affecting both physical infrastructure and cyber security. This also ensured that all key individuals had an opportunity to respond to a variety of situations to gain an excellent understanding of their responsibilities and communication protocols should an incident occur.

The Result

There were a number of objectives to this project: tying up a variety of response documents, assessing and addressing cyber security threats and improving internal and external communication protocols. Teed's experience of similar projects was hugely beneficial in enabling the consultant to identify the most effective means of collating and disseminating the required information into a workable procedure, which was then written at a level that can be understood by non-technical representatives.

Ultimately Teed's client is well placed to deal with different events without any confusion as to who is doing what, when, or how the response and recovery activity should be undertaken. Vendors and clients of the organisation are aware of what is expected of them and the project has identified actions to improve upon their own response and business continuity capabilities.

Inevitably there will always be changing threat environments to be considered and an appropriate system has been put in place to keep the response capability live and effective.

Business continuity planning considers how to deal with the consequences of an event, but at the same time it is important that the response capability is as good as it can be to ensure the consequences are minimised. No organisation wants to be reduced to working with pen and paper indefinitely or tell clients that essential trading platforms are unavailable, with all the financial client service repercussions that would ensue.