Managing the Response to Cybercrime

Background

The need for an effective response to cybercrime is becoming more urgent. No organisation is immune from failure in information security controls - from telecoms to tea shops, from supermarkets to software and game companies. Senior managers realise the implications of a cyberattack: The Information Commissioners Office (ICO) imposing fines, loss of customer confidence and damage to reputation. These things can take many years to recover from if not managed effectively. For organisations and institutions that work with highly sensitive data (such as banks and building societies), an information security breach would arguably cause even greater damage.

Whilst there is no guaranteed defence against cyberattacks, organisations need to be prepared for such an eventuality.

> The need for an effective response to cybercrime is becoming more urgent.

The Challenge

Although physical security and hardware and software solutions can work effectively, persistent cyber criminals are able to circumvent such controls. A well-known building society (referred to as 'our customer' because they would prefer to remain anonymous) realised that despite all of their controls there remains a potential vulnerability to cyberattacks. The requirement for a coherent and effective response to a cyberattack, is arguably of the utmost importance. To adequately fulfil their requirements, our customer sought the expertise of Jermyn Consulting. Our brief was to set up a realistic scenario exercise for the senior management team which simulated the events of a cyberattack.

The Solution

Jermyn Consulting are experts in scenario-based management exercises. We have designed and delivered over 200 realistic scenario exercises for customers, including bespoke cybercrime response exercises for banks and building societies.

For our customer we developed a scenario based on an extortion attempt by a hacking group that threatened to publish stolen customer data online unless a ransom was paid.

By taking part in a cybercrime scenario exercise facilitated by Jermyn Consulting, our customer's management team was able to look closely at their response mechanisms in the event of such an incident. Technical strategies were already in place so the emphasis was on developing the most effective measures to safeguard organisational reputation and customer retention. In doing so, the senior management team gained an understanding of the key stages of a response; such as detection, escalation, invocation, containment, response and recovery. These were all completed in a safe and supportive (yet realistic) environment.

The Solution Continued...

Jermyn Consulting worked with key personnel within the organisation to develop the scenario to ensure it fitted the organisation's needs, taking in to account their existing response mechanisms. Using our experience of other such exercises, we ensured pinch points were appropriately challenged.

The Outcome

The exercise enabled the management team to:

- Identify the key personnel and set up a response team with the necessary skills and knowledge.
- Confirm the response protocols and further develop their response plans.
- Identify pre-requisite actions to improve information security in general, and embed the response process.

Among the issues identified by delegates as needing attention were:

- A better understanding of the third party support services available (e.g. insurance and technical specialists).
- The need for a clear strategy of engagement with key stakeholder groups.
- The impact of social media on the organisation.
- More robust interfaces between contingency funding and major incident responses.
- Clearer decision-making powers.

Our customer now has a comprehensive action plan for fast, effective incident response in the event of a cyberattack. The future focus is on continuing to build and maintain competency within the management team to work alongside their existing effective technology solutions.

Get in Touch!

We believe all organisations can benefit from having effective management response plans and information security controls in place. If you would like to find out more about any of the concepts that have been discussed, or to find out how we can help your organisation, please do not hesitate to get in touch with us.