Cyber response planning for pension schemes

I read a fascinating article[1] on LinkedIn recently about the difference between reacting and responding. The distinction being drawn was that the former is largely unplanned, whereas the latter is planned and rehearsed. It was written by a fighter pilot, where the difference could be life and death. But the implications in many other areas were clear; **preparation is important**.

Dealing with cyber risk is topical for many organisations and pension schemes are no different. But unlike most organisations, many pension schemes do not have an incident response plan for dealing with a cyber attack.

A common reaction from trustees is that they do not know what sort of incident might have an impact on them, so how can they plan for it? It could be loss of data, systems going down, intercepted transfers of scheme funds, a ransomware demand, or something else. But despite that uncertainty, I believe that advance planning is a sensible precaution to protect a scheme and its members.

As a minimum, an incident response plan should contain a list of key contacts, available in a single place, and in all circumstances, even if your IT systems are compromised. It should include not just day-to-day contacts, but those that you would not normally need unless something goes wrong. For example, do you know how to quickly contact a suitable PR agency, the company IT director or your company incident response team?

Reference numbers are also helpful so that you are not looking for them in the middle of a crisis: your trustee indemnity policy number, your data protection registration number, bank account details etc.

A checklist of things not to forget is also helpful. For example, a list of people you might need to notify, timescales for reporting breaches to the information commissioner, some tips on dealing with media, and a reminder to have decisions properly made and documented.

Having a plan not only means that you will be able to act more effectively (i.e. respond rather than react), but that you will be able to do so more quickly.

This is important if the incident is widespread, such as a ransomware attack covering many organisations or countries. High quality cyber experts are in limited supply, and those organisations who are not able to respond quickly to an attack could find themselves at the back of the queue, with the best resources already committed elsewhere. So, if you want to have an expert available to parachute in on day one, then you may want to consider having an expert on retainer, with the terms and conditions agreed in advance.

And of course, testing your plan is important. A lot of schemes are now running table-top exercises to simulate an incident. Whilst there may be limited value in planning in detail for the specific incident you have just tested, such an exercise will inevitably highlight ideas and themes which will lead to the scheme being better prepared for any eventuality. Do not forget to include your sponsor in these exercises, and contribute your needs into their business continuity plans. This is particularly important if you use in-house resources.

In the end, an incident response plan is one of those documents that you hope you will never need. But given the prevalence of cyber risk and the amount that schemes have to lose, we believe it is well worth the investment.

Vanessa Jaeger is a senior consultant at Aon. If you would like to know more about how to tackle your cyber risks, please contact us at talktous@aon.com

By Vanessa Jaeger
Senior Consultant, Aon