How protected are your schemes against fraud and cybercrime?

Judith Hetherington explores the findings of Crowe's fifth *Governance and Risk Management Report*

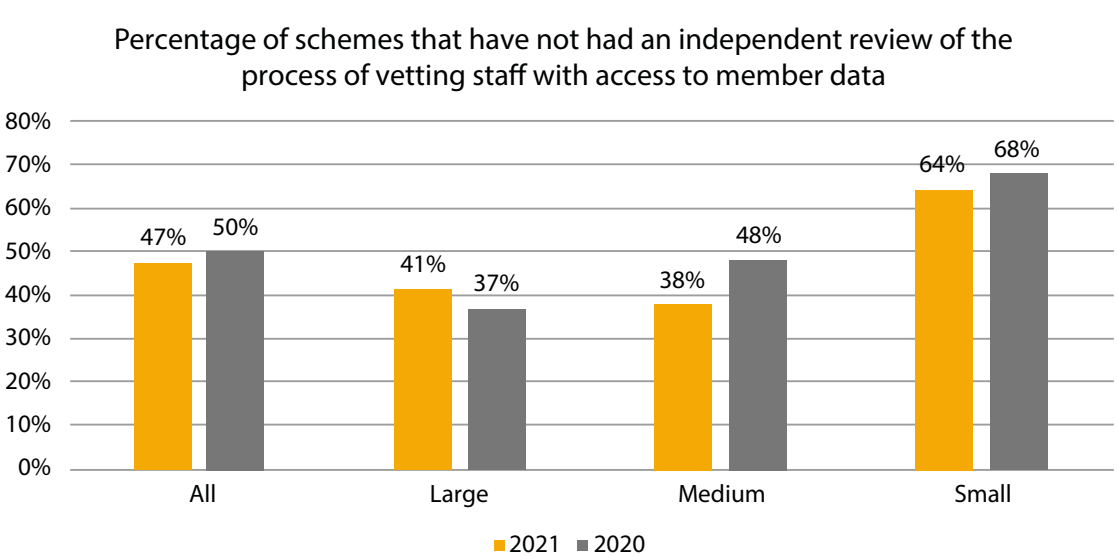
The past two years have been turbulent for many. In 2020, many service providers to pension schemes had to change their operations almost overnight to a more virtual service, and this has continued even since restrictions have been lifted. While fraud and cyber risks have always been apparent, given the changes to how suppliers have operated and the current state of the economy, there has been an increase in the attractiveness of pension scheme data to fraudsters.

Our fifth edition of the *Governance and Risk Management Report* considers some aspects of fraud and cybercrime, and we have identified some key questions for trustees to consider in regards to this.

What controls and processes does your administrator have in place to counter fraud, especially in the process of changing members' data, and how they vet new staff with access to member data?

The integrity of the people working for administrators is an important factor in preventing fraud. Even with the right controls in place, the minority of dishonest people can often identify and exploit vulnerabilities. Pre-employment vetting, and more extensive background checks for employees in positions of responsibility, is an important process to strengthen fraud resilience. Forty-seven per cent of respondents have confirmed that their administrator has not had an independent review of its process for vetting staff with access to member data prior to their appointment, to ensure it is capable of preventing fraudsters gaining access to their systems and data.

Almost half (47%) of all schemes have not undertaken an independent review of the processes for updating member details when informed of a data change. Such processes are targeted by fraudsters and are an important vulnerability that should not be left unchecked. In recent years, Crowe has seen examples of fraudsters using false information to change member details, therefore it is fundamental that trustees have assurance that the processes in place are sufficient. The survey results show that the issue is more prevalent among small schemes compared to large schemes.

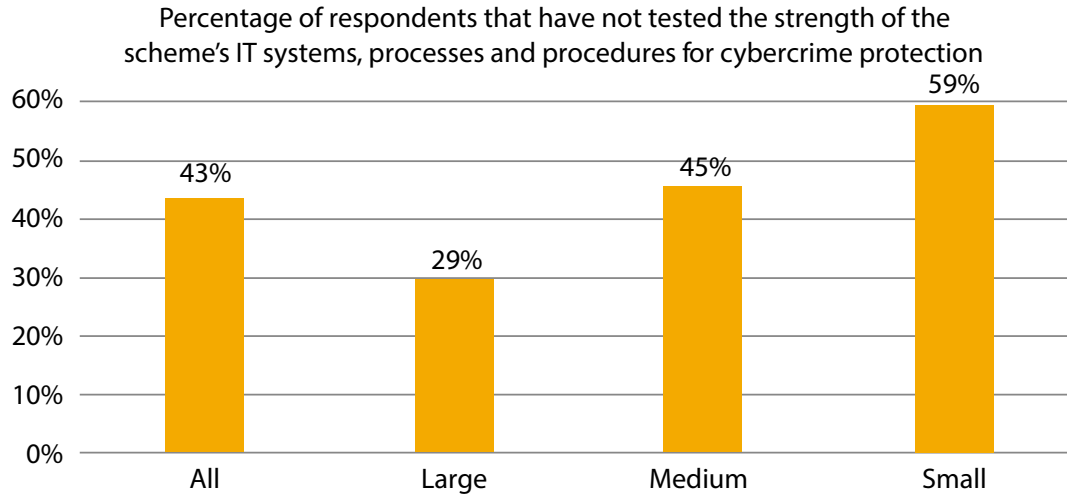


Does your administrator use electronic ID verification and if not, why not?

Twenty-nine per cent and 63% of respondents confirmed that there is no electronic ID verification for UK members and overseas members respectively. From our experience, the majority of administrators have such an ID verification system in place for UK members, but this is

less commonplace for overseas members.

Trustees should request information from their administrators concerning what system they have in place and if there is no system in place, trustees should be challenging on what plans they have for the future to put these tools in place.



Have you assessed the vulnerabilities of your suppliers to cybercrime?

The majority of pension scheme operations are outsourced to third-party providers, and as a result the majority of a scheme's cybercrime vulnerabilities will be outsourced too. The responsibility for managing cybercrime risks cannot be outsourced and remains a key part of trustee obligations. Despite this, 28% of all schemes have not assessed the vulnerability of their third-party suppliers to cybercrime. The figures range from 43% for small schemes, 33% for medium schemes, and 12% for large schemes. Over a third of pension schemes have not identified cybercrime vulnerabilities posed by third-party suppliers, and so cannot obtain assurance that the risks are being managed appropriately.

These results are concerning, especially given that cybercrime has been ranked as one of the top risks for DB and DC schemes in the previous two years and is so prevalent at present.

Are you aware of your cybercrime vulnerabilities and how cyber risks are being managed?

Forty-three per cent of respondents have not tested the cyber resilience of their scheme's IT systems, processes and procedures. The survey results show that the issue is more prevalent among small and medium schemes compared to large schemes. From review of the type of scheme that responded, the majority are administered by third-party administrators, therefore we assume that trustees have not considered it necessary to test the administrators' systems.

We recommend that trustees obtain independent assurance concerning the extent to which their administrators are cyber resilient, in accordance with the National Cyber Security Centre's (NCSC) Cyber Assessment Framework.

Do you have policies in place covering the data requirements and how this is transferred securely to all your relevant suppliers?

It is surprising to see that the only supplier where 100% of respondents confirmed that there was a policy in place was the administrator. For all other suppliers, the confirmation that there was no policy in place ranged from 1% (accounts preparer) to 21% (annuity provider).

It is imperitive that trustees review the suppliers that data is transferred to and from and a policy is put in place covering the data requirements and how this is transferred securely to the supplier.

How can Crowe help schemes with their governance and risk management?

We can see that progress has been made over the past year over the mitigation of fraud and cybercrime risks. However, there is still work to do and with the new Code of Practice that is due to be issued in October 2022, trustee boards may need to demonstrate the steps that they have done to reduce the risk of incidents of fraud and cybercrime occurring, and appropriately manage any incidents that arise. We help and support trustees by evaluating pension scheme governance arrangements, including risk management, policies and practices.

Written by Crowe pension funds partner, Judith Hetherington