Surrey Local Pension Board
5 August 2021

Cyber Security Report - Quarter 1

Background

1. The Local Pension Board requested an update on Surrey policy on cyber security and the measures being implemented to mitigate risks. This paper provides a brief update on the cyber security policies and procedures affecting both the Northern Trust, and Surrey County Council.

2. This paper begins by exploring the cyber challenges facing pension funds.

3. It considers where Surrey is now and looks at the procedures put in place by both Northern Trust and Surrey County Council to enhance cyber security.

4. The paper concludes by looking at the direction of travel and tries to identify ways in which Surrey can improve its policies and procedures.

Recommendations

5. Cyber security training for officers, Board and Committee members should be incorporated in the Fund's training plan.

6. A cyber security risk register should be created / the Administration Risk Register should be expanded in accordance with tPR recommendations.

The challenges

7. We live in a connected world and data is constantly being shared between organisations, services and individuals online. The threat of cyber-attack is already significant and it is likely to proliferate with the advent of homeworking and the security challenges posed by the Pensions Dashboard.

8. There is a multiplicity of cyber threats including ransomware attacks, denial of service, phishing and "zero-day" attacks (a vulnerability the software developer was not aware of) and they can lead to data loss, financial loss, disruption to service and reputational damage. Unfortunately, public sector organisations are not immune from cyber threats and some criminals view it as a prime target.

9. LGPS pension funds hold large amounts of exploitable personal data and assets which are an attractive target for fraudsters, scammers and cyber criminals. Funds also work with a wide range of partners, providers and suppliers that handle their sensitive data including employers, AVC providers, software providers, contractors, actuaries, lawyers, economists, and custodians.

10. Most LGPS administering authorities (circa 83%) are reliant on the host authority for cyber security. Surrey Pension Fund is reliant on the host and, although it is a circa £5 billion pension fund, it does not have the scale to justify the expense of self-contained information technology service. This means that the Fund would be competing for business continuity resources in the event of a major cyber attack on the host authority.

Northern Trust policy

11. Richard Smith and Darren Seary of Northern Trust delivered a presentation to the Pension Fund Committee in 2018. The presentation described the different cyber security risks, with an emphasis on ransomware and the ways in which it was being dealt with at Northern Trust.

12. A brief summary of the presentation is provided below:

    a. Richard provided a brief overview of Northern Trust's financial stability and global reach and the importance of those to protecting client assets.

    b. He highlighted the increasing focus on contingency planning and enhanced cyber security for our clients.

    c. Darren, a Senior VP in NT's Information Security and Technology Risk Management Team, gave an overview of the threat landscape facing financial institutions including Ransomware, Social Engineering and DDOS attacks.

    d. He discussed the controls NT has in place to both proactively and reactively identify and respond to cyber threats.

    e. He outlined NT's IT governance, information security risk management and how its protocols are regulated and tested.

Surrey's policy

13. SCC takes a wide-ranging approach to cyber security. This has been demonstrated by the attainment of numerous security certifications including:

    a. PCI DSS from the Payment Card Industry SAQ-C

    b. PSN Certificate – Public Sector Network security standard

    c. IG Statement of Compliance – NHS Information Security Standard (N3)

    d. ISO 27001 – Information standard for Information Security Management Systems

14. SCC regularly reviews its accreditations and Surrey are planning to add to the list by undertaking assessment and certification for the National Cyber Security Centre's Cyber Essentials programme.

15. SCC PSN certification requires annual independent penetration testing across the network and covers user endpoint devices, servers, solutions such as our remote access/VPN, analysis of network devices such as firewall and our policies.

16. SCC has a robust set of IT Security and Information policies, and staff must undertake e-learning training. Policies are regularly reviewed and adjusted in accordance with new research and industry best practice; for example, Surrey are widening the use of multi-factor authentication for external access to systems and increased the password length requirements while stopping the requirement for staff to regularly change passwords.

17. There is a comprehensive risk assessment process for new IT solutions as well as regular assessment of existing solutions. Independent Penetration Testing is carried out where necessary to provide assurance of Surrey's and our partners' infrastructure.

18. There are many technical and operational controls in place to proactively prevent, detect and, if necessary, recover from cyber incidents.

19. SCC deploy multiple firewalls and boundary controls including web filtering. There are numerous alerting and monitoring tools including a SIEM and SOC, a web application firewall that protects our public facing sites. Surrey provides resilience and recovery through load balancers, replication across data centres and backup tools, and desktop anti-virus is deployed across the whole estate.

20. E-mail represents one of the biggest attack vectors globally and it has recently been the entry point for most ransomware outbreaks. In order to combat this, Surrey has multiple layers of defences covering reputation, spam, content and virus filtering. Surrey deploys multiple antivirus engines in addition to leveraging the security and scanning provided by Microsoft's O365 filtering.

21. Many threats still leverage known vulnerabilities that have not been fixed. SCC follow a regular patching programme for all devices and infrastructure across the network, makes use of industry standard deployment tools and has a working group that identifies improvements and efficiencies that can be made in this area.

Surrey's internal controls

22. Surrey County Council (SCC) uses an up-to-date, cloud-based version of Logotech Treasury Management software.

Logotech's treasury management provides greater controls, for example:

- Information only needs to be entered once, providing less opportunity for user input error (as well as increasing efficiency).

- Logotech has individual user accounts, which are accessed with a password. This ensures access is tightly controlled.

- There is an audit log within the Logotech system, which cannot be edited and provides a record as to each user's activity within the system, increasing accountability for actions taken.

- Permissions associated with user accounts can be customised. For example, different users have different financial limits where approval is required, and this can be reflected in Logotech.

- The Councils' strategic information can also be incorporated into the system. For example, if there is a limit to an investment amount, this can also be reflected in Logotech so the system will not accept a breach.

23. Payments made by the Pension Fund are subject to strong internal controls and separation of duties. Payments raised by one officer must be authorised by (at least) one other officer and the quantum of the payment determines the seniority of the officer required to approve it. For example, the Strategic Finance Manager (Pensions) can authorise invoices of up to £25,000 and, above that, only the Director of Corporate Finance Resources can approve it.

Horizon scanning

24. The key actions that should be taken / reinforced in order to build up cyber resilience and ensure effective management of risks.

    a. Undertake training in order to gain an understanding of the Fund's cyber security approach and its recovery plan

    b. Understand the reach of the Fund's cyber footprint - including collaboration with external partners

    c. Engage with the host council to understand the current cyber security arrangements and where the Fund fits into these

    d. Review the Fund's governance arrangements and polices to incorporate the evolving cyber risk

    e. Ensure the administration function has robust business continuity / incidence response plans in place which are known to key officers, Board and Committee members

The Pension Regulator's view

25. Surrey, in common with many LGPS funds, is heavily reliant on the host authority for its security systems and, although this is not optimal, tPR believes that it need not be a problem as long as the managers have a good understanding of the IT systems in place and have given careful consideration to the risks of cyber crime.

26. Scheme managers should be aware of the risks associated with cyber crime and have robust resilience procedures in place and maintain and review a cyber risk register.

27. Scheme managers and pension boards should understand the risks posed to data and assets held by the fund so that steps can be taken to mitigate them and this should be reflected in the risk register.

28. Regular independent penetration testing should be carried out and scheme managers should consider physical security as well as protection against remote attacks.

29. Scheme managers should be aware of the cyber security processes used by third party providers, such as the actuary or the custodian, that handle fund assets or data.

30. The Pension Regulator has published "Cyber security principles for pension schemes" as part of Code of Practice 14, which will be assimilated into the Single Code in Due Course.

Final observations

31. Pension funds will need to be nimble in order to address the cyber risks posed by large numbers of staff working from home.

32. Although the gateway to the Pensions Dashboard eco system should not challenge Surrey's cyber security in itself, mediocre security controlling members' access may presage a surge in transfer requests and identity fraud.

Report contact: John Smith

Contact details: T: 0208 213 2700 E: john.smith@surreycc.gov.uk

Sources/background papers:

1. Northern Trust Cyber Security

2. SCC Cyber Security Policy (condensed)

Annex

Security Principles for Pension Schemes – tPR publication copy of webpage:(https://www.thepensionsregulator.gov.uk/en/document-library/regulatory-guidance/cyber-security-principles-the-pensions-regulator#main)

This page is intentionally left blank