The Surrey Local Pension Board
25 July 2018

Cyber Security

Background

1. The committee requested an update on Surrey policy on cyber security and what is being implemented to mitigate the risk. This paper provides a brief update on the cyber security policies and procedures affecting both the Northern Trust, and the Surrey County Council.

2. Following the request, this paper covers procedures in place by both the Northern Trust and Surrey county council on cyber security.

Northern Trust policy

3. Last year, the pension fund committee received a presentation from Richard Smith and Darren Seary of Northern Trust which described different cyber security risks, with an emphasis on ransomware, and the ways in which this was being dealt with at Northern Trust. The presentation is included in Annex 1.

4. A brief summary of the presentation is provided below:
   - Richard Smith provided a brief overview of Northern Trust's financial stability and global reach and the importance of those to protecting client assets.
   - RS spoke about increasing focus on contingency planning and cyber security to our clients and introduced Darren Seary, Senior VP in NT's Information Security and Technology Risk Management team.
   - DS gave an overview of the threat landscape facing financial institutions, including Ransomware, Social Engineering and DDOS attacks.
   - DS spoke about the controls NT has in place to proactively and reactively identify and respond to cyber threats.
   - DS spoke about NT's governance around IT and Info security Risk, and how it is regulated and tested.

Surrey policy

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

- PCI DSS from the Payment Card Industry SAQ-C
- PSN Certificate – Public Sector Network security standard
- IG Statement of Compliance – NHS Information Security Standard (N3)
- ISO 27001 – Information standard for Information Security Management Systems

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

7. 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.

8. 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.

9. 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, or our partners' infrastructure.

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

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

12. Email still represents one of the largest attack vectors globally and recently has been the entry point for most ransomware outbreaks. To combat this Surrey have multiple layers of defences covering reputation filtering, spam, content and virus filtering. Surrey deploys multiple antivirus engines in addition to leveraging the security and scanning provided by Microsoft's O365 filtering.

13. 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, make use of industry standard deployment tools and have a working group that identify improvements and efficiencies that can be made in this area.

Report contact: Ayaz Malik, Pensions Accountant Advisor (Investments, Funding & Governance)

Contact details: T: 020 8541 9705 E: ayaz.malik@surreycc.gov.uk

Sources/background papers:

Annexes:

1. Norther Trust Cyber Security Policy
2. SCC cyber security policy

This page is intentionally left blank