City of BRADFORD METROPOLITAN DISTRICT COUNCIL

Report of the Managing Director, West Yorkshire Pension Fund to the meeting of Local Pension Board to be held on 21 March 2023.

AM

Subject: Cyber Security

Summary statement:

Cyber attacks and threats are one of the biggest challenge organisations, like WYPF, face today. Cyber attacks in recent times have become more specialised and criminals are focusing now on using deceptive techniques to target individuals.

This growing trend of attacks have resulted in significant damages to organisations that not only includes financial losses and operational disruptions, but also significant reputational damage. In the light of current regulation (e.g. General Data Protection Regulation), these risks become particularly relevant for organisations that store financial information and personal identifiable information about individuals, as is the case for WYPF.

Staff working from home has increased cyber security fears as it is much harder to keep an eye on everyone.

Cyber readiness of WYPF (led by Bradford Council) is therefore vital in aiding the ability to detect, prevent, contain and respond to evolving threats in the digital environment, which have had a severe effect in similar institutions

EQUALITY & DIVERSITY:

None.

Euan Miller
Managing Director

Portfolio: Leader of Council & Corporate

Report Contact: Yunus Gajra
Assistant Director (Finance, Administration and Governance)
Phone: (01274) 432343
E-mail: yunus.gajra@bradford.gov.uk

Overview & Scrutiny Area: Corporate

1.0 BACKGROUND

1.1 Cyber security consists of technologies, processes and controls designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks and protects against the unauthorised exploitation of systems, networks and technologies.

1.2 The global cyber security landscape has seen increased threats in recent years. Through the pandemic, cyber criminals took advantage of misaligned networks as businesses moved to remote work environments. In 2020, malware attacks increased 358% compared to 2019.

1.3 From here, cyber attacks globally increased by 125% through 2021, and increasing volumes of cyber attacks continued to threaten businesses and individuals in 2022.

1.4 Russia's invasion of Ukraine has had a massive impact on the cyber threat landscape. Since the start of the war, Russian-based phishing attacks against email addresses of European and US-based businesses have increased 8-fold. Nearly 3.6 million Russian internet users have also experienced breaches in the first quarter of 2022, an 11% increase quarter-on-quarter.

2.0 Why is cyber security important?

2.1 With the GDPR (General Data Protection Regulations) now in force, organisations could be faced with fines of up to €20 million or 4% of annual global turnover for certain infractions. There are also non-financial costs to be considered, such as reputational damage and loss of customer trust.

2.2 Cyber attacks have become more sophisticated with attackers using an ever-growing variety of tactics to exploit vulnerabilities, such as social engineering, malware and ransomware.

3.0 What are the consequences of a cyber attack?

3.1 Cyber attacks can disrupt and cause considerable financial and reputational damage to even the most resilient organisation like WYPF. If we suffer a cyber attack, we stand to lose assets, reputation and business, as well as, potentially, fines and litigation.

4.0 Types of cyber security threats

4.1 Ransomware

One of the fastest growing forms of cyber attack, ransomware, is a type of malware that demands payment after encrypting the victim's files, making them inaccessible. Paying the ransom does not guarantee the recovery of all encrypted data.

4.2 Phishing

Phishing attacks are continually on the rise. Often indistinguishable from genuine emails, text messages or phone calls, these scams can inflict enormous damage

organisations.

Bradford Council captures and blocks approximately 65,000 spam emails each month to prevent them from arriving in inboxes but the originators of these types of email are constantly evolving their methods and despite us being up to date with the latest IT security systems and filters occasionally staff may still receive one. Some of these emails are easy to identify because they have odd looking subject titles or sender email addresses, however, some spam emails are less easy to detect and even when opened can look legitimate.

4.3 Malware

Malware is a broad term used to describe any file or programme intended to harm a computer, and encompasses trojans, social engineering, worms, viruses and spyware.

4.4 Social Engineering

Social engineering is used to deceive and manipulate victims to gain computer access. This is achieved by tricking users into clicking malicious links or by physically gaining access to a computer through deception.

4.5 Outdated Software

The use of outdated (unpatched) or unsupported software (e.g. Microsoft XP) opens up opportunities for criminal hackers to take advantage of known vulnerabilities that can bring entire systems down.

4.6 Vulnerabilities in web applications and networks

Cyber criminals are constantly identifying new vulnerabilities in systems, networks or applications to exploit. These activities are conducted via automated attacks and can affect anyone, anywhere

5 Elements of Cyber Security

5.1 Application Security

Web application vulnerabilities are a common point of intrusion for cyber criminals. As applications play an increasingly critical role in business, organisations urgently need to focus on web application security to protect their customers, their interests and their assets. WYPF's applications are thoroughly tested and access is by user registration and passwords.

5.2 Information security

Information is at the heart of our business, whether it's business records, personal data or intellectual property. ISO 27001:2013 (ISO 27001) is the international standard that provides the specification for a best-practice information security management system (ISMS). WYPF has gained accreditation for this standard.

5.3 Network Security

Network security is the process of protecting the usability and integrity of your network and data. This is usually achieved by conducting a network penetration test, which aims to assess our network for vulnerabilities and security issues in servers, hosts, devices and network services. Regular installation of patches is done by Bradford Council and WYPF to ensure that any bugs are fixed. WYPF has successfully carried out penetration testing on our systems and will continue to do so on a regular basis.

5.4 Business Continuity Planning

Business continuity planning (BCP) involves being prepared for disruption by identifying potential threats early and analysing how day-to-day operations may be affected. WYPF has a full BCP in place.

5.5 End-user education

Human error remains the leading cause of data breaches, Bradford Council has a number of IT policies in place to ensure that every employee is aware of the potential threats they face, whether it's a phishing email, sharing passwords or using an insecure network. Staff are required to undergo mandatory security training annually.

5.6 Investment in Infrastructure

WYPF has invested heavily in upgrading our server hardware and infrastructure to ensure that it is compliant with the latest technology and ensure security risks are minimised.

5.7 Recent Cyber attacks

- In January 2022, KP Snacks suffered a ransomware attack. The company was unable to 'safely process orders or dispatch goods' as a result of the attack. As a result, supply chain issues continued until the end of March. It is likely a ransom was paid.

- An attack on 4 August 2022 caused widespread outages across the NHS. The target was Advanced, a company that provides software for various parts of the health service. It affected services including patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services and emergency prescriptions.

- Over 170 email addresses of customers were mistakenly copied into an email by the UK Home Office's visa service in April. An email was sent to inform the customer that their appointment time had been changed. Emails included in this breach were both personal and those sent by lawyers on behalf of clients. It is likely that the breach was caused by a malicious insider.

- In January 2023 Royal Mail was hit by cyber attack by a Russian linked ransomware gang, which caused "severe disruption" to its international export services. It was unable to dispatch items, including letters and parcels, overseas, however domestic mail was not affected. It took six weeks to resume full international service.

6.0 WYPF (CBMDC – City of Bradford Metropolitan District Council) controls in place

WYPF takes a wide-ranging approach to cyber security. This has been demonstrated by:

- ISO 27001 – Information standard for Information Security Management Systems
- PSN Certificate – Public Sector Network security standard
- WYPF/CBMDC have 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, CBMDC are widening the use of multi-factor authentication for external access to systems.
- 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 WYPF's infrastructure.
- CBMDC deploy multiple firewalls and boundary controls including web filtering. There are numerous alerting and monitoring tools, a web application firewall that protects our public facing sites. CBMDC provides resilience and recovery through load balancers, replication across data centres and backup tools, and desktop anti-virus is deployed across the whole estate.
- 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, CBMDC has multiple layers of defences covering reputation, spam, content and virus filtering. CBMDC deploys multiple antivirus engines in addition to leveraging the security and scanning provided by Microsoft's O365 filtering.
- Many threats still leverage known vulnerabilities that have not been fixed. CBMDC follow a regular patching programme for all devices and infrastructure across the network and makes use of industry standard deployment tools.

7.0 Horizon scanning

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

8.0 The Pension Regulator's view

8.1 WYPF, 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.

8.2 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.

8.3 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.

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

8.5 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.

8.6 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.

9.0 Training

9.1 WYPF is currently finalising a training plan for Board and Committee members. Cyber security will be incorporated into that training plan.

10.0 OTHER CONSIDERATIONS

None

11.0 FINANCIAL & RESOURCE APPRAISAL

WYPF's training budget for 2023/24 incorporates costs for member training, which includes cyber training.

12.0 RISK MANAGEMENT AND GOVERNANCE ISSUES

Cyber risk is identified in WYPF's risk management register and has a D2 Amber rating (Likelihood Low, Impact Critical).

13.0. LEGAL APPRAISAL

None

14.0. OTHER IMPLICATIONS

14.1 SUSTAINABILITY IMPLICATIONS

None

14.2 GREENHOUSE GAS EMISSIONS IMPACTS

None

14.3 COMMUNITY SAFETY IMPLICATIONS

None

14.4 HUMAN RIGHTS ACT

None

14.5 TRADE UNION

None

15.0. NOT FOR PUBLICATION DOCUMENTS

None

16. RECOMMENDATIONS

It is recommended that the report is noted.

17. APPENDICES

Appendix A – The Pensions Regulator – Cyber Security Principles.

18. BACKGROUND DOCUMENTS

None