BRECKLAND DISTRICT COUNCIL

Report of: Jane James, Executive Member for Customer & Corporate Services

To: Overview & Scrutiny Commission 01 December 2022

Authors: Ben Meen – IT & Digital Manager
Adele Newsome – Customer Experience Manager

Subject: IT Security & AI Data Protection Overview

Purpose: To provide members of the commission with an overview the Council's data security infrastructure and approach to the use artificial intelligence (AI) technologies.

Recommendation

Members of the commission are asked to note the report.

1.0 BACKGROUND

1.1 This report seeks to provide Members with an overview of the Council's approach to the security of its IT systems and some further information regarding data handling within the Council's approach to the use of artificial intelligence (AI). The report seeks to provide insight into the systems, approaches, and audits to provide assurance that we are delivering our digital services in a safe, compliant, and ethical way.

1.2 IT security was a specific request from the Commission and features on the workplan. The AI element of the report is a follow-up to a previous report provided to the Commission earlier in the year.

2.0 IT SECURITY

2.1 Cyber crime is estimated to cost the world 1% of GDP (gross domestic product) every year. It is a constantly evolving and rapidly expanding area of threat to any business of any size, but particularly to public sector bodies who are increasingly finding themselves targets of sophisticated state-sponsored hackers seeking to steal data and disrupt public life.

2.2 Every month the Council's IT service blocks around 57 million unauthorised probes of its systems, which translates to around 22 every single second. In the time it's taken you to read the beginning of this report we will have already defended ourselves against over 200 of these attacks.

2.3 The impact of these attacks can be devastating, with the average cost of a breach to a small business being £120k - £1m. Reputational damage is another key consideration with a recent report highlighting that a 'reputation premium' is associated with some brands and services, and that a cyber attack can fundamentally undermine this trust and have an impact on the bottom line that can be as high as 25% of revenue[1]

[1] Aon & Pentland Analytics, https://www.aon.com/reputation-risk-cyber-social-media-pentland-analytics-aon/index.html

2.4 As a Council, our residents and partners trust that we will manage their information in a secure way and any significant cyber breach would significantly undermine this confidence and impact our ability to deliver services in the future.

2.2 As cyber criminals get more sophisticated, both the technology used to launch and defend against cyber attacks evolves resulting in increasingly innovative types of attack. Some of the most common forms of attack include;

- **Phishing** - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

- **Distributed Denial-of-Service** - targeting systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

- **Malware** - refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans. These can often lay dormant for months or even years before being activated.

  The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

2.3 In order to defend against this ever-changing landscape of attacks, it's important that the Council has a multi-layered approach to defence. This approach ensures that should any one layer fail to defend against an attack, whether by innovative attack design or service failure, that there are multiple other layers of defence that are still able to prevent the attack.

2.4 This is important, because as the Council faces such a high volume of daily attacks and these are constantly evolving to try and outpace our security, it's the multiple layers that allow us to stay ahead.

2.5 These layers (which are further defined in Appendix A) are broadly split between:

- **Physical security** - such as door security, CCTV and alarm systems that prevent access to our hardware and systems. This is both for data hosted on our premises and for data hosted by third parties (i.e. in the cloud).

- **Digital security** - including everything from firewalls that digitally detect and prevent unrecognised access to our systems through to policies that prevent access from certain countries and ensure that devices are kept up to date.

- **User education** – one of the most important and primary lines of defence is educating users of Breckland systems on how to identify and respond to threats. Even organisations with the most sophisticated digital and physical systems will not be able to prevent creative phishing attacks that may come in via email, phone or any other communication channel.

2.4 The Council's approach to cyber security is validated annually through a Public Services Network (PSN) audit. Undertaken by the Cabinet Office, this is a recognised, externally accredited and cross-governmental set of assurance standards that ensure that our approach to cyber security is resilient, secure and in line with best practice. The Council has

held this accreditation for a number of years and continues to remain compliant with the most recent audit taking place earlier in the year.

2.5 Cyber security is, however, a constantly moving and evolving thing which is why as a Council we are continuously evaluating our approach, incorporating lessons learned and evaluating emerging approaches and technologies between audits to ensure we keep ahead of attackers.

2.6 Some of the projects that are currently underway to enhance our approach are detailed in Appendix B and cover a range of areas across all layers of security.

2.7 Whilst this should give comfort that our approach is resilient, adaptive and in line with best practice, it is vital that we ensure everyone that engages with the Council takes an element of responsibility for cyber security, whether directly as a user of our IT services or a recipient of Breckland-controlled data.

2.8 By remaining vigilant, informed and alert to threats can we continue to maintain secure systems for the benefit of our residents.

3.0 CHATBOT / ARTIFICIAL INTELLIGENCE (AI) APPROACH

3.1 Our approach to the use of AI is to add additional access channels that are available 24/7 to enable our customers to access information. This is in addition to our current customer access channels of phone, webchat and face-to-face.

3.2 Throughout the implementation of the use of AI a Data Protection Impact Assessment (DPIA) has been carried out every time any new functionality is added on (such as Alexa). The DPIA is drafted in consultation with the Council's Data Protection Officer and is signed off by both the Data Protection Officer and the Senior Information Risk Officer.

3.3 As part of the DPIA process we review our privacy notices: the Customer Contact Centre Privacy Notice (which is available at https://www.breckland.gov.uk/privacy/customer-contact-centre) states why the Council needs personal data. It is required to be able to answer queries and process service requests. With the introduction of Bobbie and Alexa this doesn't change and is still the appropriate reason.

3.4 However, the Customer Contact Centre Privacy Notice has been revised regarding the retention of the customer transcripts for use by our chatbot. These are retained for monitoring and training purposes within the chatbot content management system for 183 days / 6 months. This aligns with the Council's data retention practices for its existing channels. It is also in line with standard practice to ensure information is available for any complaint investigations. We would reasonably expect a customer to complain within 6 months and therefore it is set to the same time period.

3.5 Before we publicly release the Breckland Council Assistant - Alexa Skill, there will be a full review of the Customer Contract Centre Privacy Notice to include all the relevant information for the Breckland Assistant - Alexa Skill. This will be undertaken in consultation with the Council's Data Protection Officer.

3.6 Customers must accept the privacy policy before they can use the Council's chatbot. When accepting, there is a link to the Customer Contact Centre Privacy Notice which includes what their information is used for and how long it will be stored. There is also access to any 3rd party's privacy notices. The Council's suppliers (in relation to Customer services) process data in accordance with our instructions and have a contractual agreement with us to do

so. Therefore, the customer is not required to accept a 3rd parties privacy policy. For customers already using an Alexa device, they would have to have signed up to the Alexa privacy policy to be able to use Alexa; in future, if they wish to later add the Breckland Council Assistant - Alexa skill they would be presented with information about the skill and how to use it, including links to access our privacy policy.

3.7 All contact channels are built with customer options to allow customers to delete their data outside the normal retention periods. For example, the Council's chatbot has within its settings a deletion option, with a warning that this is permanent. Within the Breckland Council Assistant – Alexa skill, if a customer asked 'what does Breckland do with my data' it would link to a response, which asks you to confirm, again, as this is permanent before the data is deleted from the chatbot content management system.

3.8 No personal data is passed from the chatbot content management system back to the Alexa system; information that is passed back is a response to a question which is information that is currently available on our website.

3.9 Customer transcripts and voice recordings are stored within our 3rd party contracted systems, Ubisend (Chatbot & Alexa Skill) and Mitel (Telephony). These systems are securely passworded for access and all have retention periods set for 6 months to enable access to recordings / transcripts for the purposes of complaint investigation, along with training. Within the Alexa platform the customer's voice recordings retention periods are managed by the customer as per the Alexa privacy notice.

3.10 Currently the Ubisend system can learn from customer questions; these questions are developed by an agent, by assigning the question to a relevant frequently asked question (FAQ) and any questions that come into the system that contain personal information inputted by the customer are disregarded and deleted in line with the retention policy. Development by the agent, combined with Natural Language Processing (NLP), helps the chatbot get better at selecting the right response for the customer, but there is no personal data retained within the training section.
Note – Natural language processing (NLP) is ***the ability of a computer program to understand human language as it is spoken and written*** *-- referred to as natural language. It is a component of artificial intelligence (AI).*

3.11 In terms of further machine learning and automated decision making, the Council is not currently working or developing this. If/when we do so, due consideration would be given to data security at that time.

4.0 OPTIONS

4.1 To note the contents of the report.

5.0 EXPECTED BENEFITS

5.1 To provide members of the Commission a clear overview of how the Council approaches IT security and the use of artificial intelligence technologies.

6.0 IMPLICATIONS

6.1 Corporate Priorities

- Working Smarter

6.2 Data Protection

6.3 Data protection is key to the Council's IT security and use of AI.

7.0 WARDS/COMMUNIITES AFFECTED

7.1 All wards.

8.0 ACRONYMS

7.1 Acronyms are defined within the main body of the report.

Background papers: Overview & Scrutiny Commission Minutes 26 May 2022, minute ref 35/22

Lead Contact Officer
Name and Post: Ben Meen – IT & Digital Manager
Adele Newsome – Customer Experience Manager
Telephone Number:
Email: ben.meen@breckland.gov.uk
Adele.newsome@breckland.gov.uk

Key Decision: No

Exempt Decision: No

This report refers to a Discretionary Service

Appendices attached to this report:

Appendix A	Cyber Security Defence Overview
Appendix B	List of planned Cyber Security Projects