Protecting the Council's Data and Information Assets

Data and Cyber Briefing

Audit Committee – 18th October 2022

Cheryl Doran, CIO and Assistant Director for IT and Digital

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council

Contents

- Data accountabilities
  - GDPR
  - IAB

- Loss of Data; where the risks come from and their impacts
  - Cyber attacks
  - People
  - Process
  - Technology

- Mitigating our risks – key activities and processes

Our duties to protect citizens data

DATA ACCOUNTABILITIES

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council

Data Breach Obligations

- The UK General Data Protection Regulations (UK GDPR) introduced a new legal obligation to report breaches which result in loss of personal data to the Information Commissioner's Office (ICO). The UK GDPR defines 'personal data breach' in Article 4(12) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
- There has been a total of 191 data breaches reported over the past year against 144 for the previous year (2020/2021). There were **zero** personal data breach has been notified to the ICO during this period 2021-2022.

Accountability approach

- The Information Assurance Board (IAB), chaired by the Senior Information Risk Owner (Director Digital & Customer Services), co-ordinates the Council's activities in managing its obligations in respect of data protection. It meets quarterly and it provides a quarterly report to CLT and Deputy Leader on its programme of work.
- IAB members include senior representation from IT&D, Legal Services, Public Health, HR Birmingham Audit and Procurement.
- It works on a thematic basis which includes updates on Incident Response Management, Regulatory Compliance, Information Security and Training and Awareness.

Understanding where the risks come from and their impacts

LOSS OF DATA

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council

Cyber Attacks

- **Most Likely =** A ransomware attack by a very capable organised criminal group specifically targeted at Birmingham City Council for financial gain. This can result in loss of data, or service disruption/inability to access ad hoc systems
- **Most Dangerous** = A targeted cyber-attack by the most capable nation-state or proxy threat actors, seeking to sabotage the delivery of all services to Birmingham City Council

Cyber attacks – Some examples

- **MALWARE** - Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system and can compromise data/sensitive information. Examples include Ransomware, Key loggers, Trojans, Bots, Spyware, Worms and Viruses
- **RANSOMWARE** - A common type of malware that prevents one from accessing their system. The system itself may become locked, data stolen, deleted or encrypted unless ransom is paid. This can spread across multiple systems in an organisation causing immense damage and loss of data
- **PHISHING** – Deceptive/malicious communications that appears to originate from credible sources. Through phishing, attackers can gain access to systems, compromise data/sensitive information.
- **PASSWORD COMPROMISE** – Passwords provide the first line of defence against unauthorised access to sensitive data held on the council's IT network. If one's password is unintentionally divulged to a cyber-criminal or they have been able to crack it due to weak passwords, they can gain access to the council's network and lead to data compromise/loss.
- **DOS/DDOS** - This type of attack floods the target system with a huge amount of traffic that exhausts the bandwidth of a system. This can bring down the system/network and prevent access to critical information/data.
- **SOCIAL ENGINEERING** – Cyber criminals use social engineering to trick people into carrying out certain actions, such as divulging confidential information from which they can gain access to IT systems and sensitive data.

People

- Of the 191 data breaches reported during 2021/2022, 83 were designated as 'Unauthorised Disclosure'. This is where personal data has been disclosed to an unauthorised to third party.
- A further 100 data breaches were designated as 'Email Disclosure' where information had been sent to the incorrect email addresses
- Analysis of the nature of the breaches shows that many of these breaches are because of human error.

Process

- The ICO must be notified of a data breach within 72 hours of the council becoming aware of the breach. Time starts from the moment the council becomes aware of the breach.
  - a personal data breach must be reported to the ICO if it's likely to result in a risk to people's rights and freedoms.
  - if the data breach is likely to result in a risk to people's rights and freedoms, the individuals who have been affected must be informed.
  - the risk has to be assessed on a case-by-case basis.
- Staff are required to report immediately after they become aware of the data breach, by completing a Personal Data Security Breach Notification form.
- Serious data breach incidents are referred to the Strategic Director or Monitoring Officer to determine the next course of action for notifying the (ICO).

Technology - Where risks can come from

- Legacy Devices and systems where vulnerabilities can be exploited
- Unpatched systems that if not kept up to date can be exploited
- Lack of defenses through inadequate early detection and monitoring tools and capabilities which can identify threats/vulnerabilities and prevent unauthorized access/compromise
- Inadequate resources to manage existing technologies
- Poor controls over assets that could potentially leave data prone to exploitation
- Weak password policies and access control which can allow exploitation resulting in data compromise.
- Weak network control/management
- Lack of ability to recover in the event of a cyber attack

Activities, programmes and work practices to reduce data risks

RISK MITIGATION

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council

Process

- Thematic work in the Information Assurance plan
- Data Protection Impact Assessments
- Information Asset registers
- IAB has regular updates; representation from across the Council (Legal, HR, Service areas, IT)
- Maturity model for our information management has been in place and we have improved from 1/5 to 3/5 in the last two years.
- Lessons learned from serious data breaches and monitoring responses

Cyber attacks

Actions are split into two types

- Reducing the likelihood of the risk
  - Better awareness amongst the organisation of the various threats through awareness campaigns and training
  - Patching and maintaining software to eliminate vulnerabilities

These actions manage the risk and protect us against attack

- Minimising the impact of the risks
  - Software and a security operations centre to detect incidents early
  - Offline and immutable back ups to be able to recover quickly in the event of a cyber attack.

These actions minimise how much damage or downtime impacts on our operations in supporting our customers

People

- To mitigate risks, there is a programme of training and awareness that can be accessed by staff as well as technical measures that are in place to tackle high risk activity. Examples include:
  - 93% (27/29) Information Asset Owners (AD's only) completed training
  - 8171 (85%) Employees completed cyber security training as part of the mandatory bundle launched April 2021
  - 37 Different courses within the "Your Development" corporate offer mapped against the "Value Our Information" behaviour
  - New Ways of Working workshops, sub-groups, focus groups and bulletins bring together consistent message regarding safety and security of data when hybrid working

Technologies

- We have implemented new software to support us in preventing, detecting and managing cyber security incidents
- There are new password controls to make it harder for hackers to penetrate our systems
- We continue to have regular patching and updates to our systems to protect us from security vulnerabilities
- We have implemented new systems to ensure that we can recover our data and systems quickly in the event we are attacked.

CURRENT RISK POSITION

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council

Current risk position

- Improving position for our strategic risks – moved from significant to material
- Our activities have reduced risk impact, particularly our monitoring software, operations centre for early detection and the back up software that enables us to have a copy of our data locked away offline to recover in the event of a cyber attack.
- Improved password strength and multi-factor authentication reduces likelihood of both data loss and cyber attack
- The activities we are taking around educating people have an impact on likelihood for both risks, these are activities we need to constantly refresh as – it only take one person to make a mistake that could let cyber attackers in or cause a data breach.

@BhamCityCouncil

@birminghamcitycouncil

@birminghamcitycouncil

birmingham.gov.uk

BE BOLD BE BIRMINGHAM

BIRMINGHAM 2022 commonwealth games

PROUD HOST CITY

Birmingham City Council