Information Governance Management

Annual Report 2021

Senior Information Risk Owner

July 2020 -
June 2021

1 Introduction

1.1 The Council's Audit, Risk and Scrutiny Committee agreed the Council's revised and updated Information Governance Management & Reporting Framework in September 2016; as part of this the Committee agreed to receive an annual report in relation to the Council's information governance assurance. This is the fifth of these reports being presented to Committee.

1.2 This report collates, analyses and monitors the Council's performance in relation to freedom of information, data protection and information security, to give assurance that trends, issues, incidents, and breaches are dealt with appropriately as they arise.

1.3 Ensuring the proper use and governance of the Council's information and data is an ongoing activity. New and changing legislation, systems, staff, and ways of doing business, as well as new and emerging cyber threats, all shape and change the environment within which the Council operates in relation to effective use and governance of its information and data.

1.4 Keeping up means a careful balancing between the requirement to monitor and be adaptable to our changing environment, and the requirement to agree and implement assurance improvements over the medium term.

1.5 To this end, actions to improve assurance in the medium term are identified, actioned and monitored through the Information Governance and Cyber Security risks on the Corporate Risk Register; regular updates on which are reported separately to the Council's Audit, Risk & Scrutiny Committee.

1.6 The Council's Information Governance arrangements were subject to Internal Audit, reported in February 2020. The objective of the audit was to provide assurance that the Council has adequate controls in place to mitigate the risks identified in the Corporate Risk Register and that these controls are operating as expected. The audit found that comprehensive and clear policies, procedures and mandatory training are in place and that corporate risk and related controls are being monitored by the Information Governance Group, chaired by the Council's Senior Information Risk Owner, with exception reporting to Corporate Management Team. Information Governance controls were found to be comprehensive and control assessments generally well-supported.

1.7 The National Records of Scotland, Public Records (Scotland) Act (PRSA) 2011 Assessment Team, assessed the Council's annual update of its arrangements under the Act in May 2020. The Assessment Team found that the Council continues to take its statutory obligations seriously and maintains the required records management arrangements in full compliance with the Act.

2. Information Governance Performance Information July 2020 - June 2021

2.1 Data Protection Rights Requests

Fig 1: Annual number of requests received

Type of Request ▲	12 months to June 2021	12 months to June 2020
Subject Access	281	234
Third Party	407	521
Other Rights Request	21	16

Fig 2: Requests received in the 12 month to end June 2021

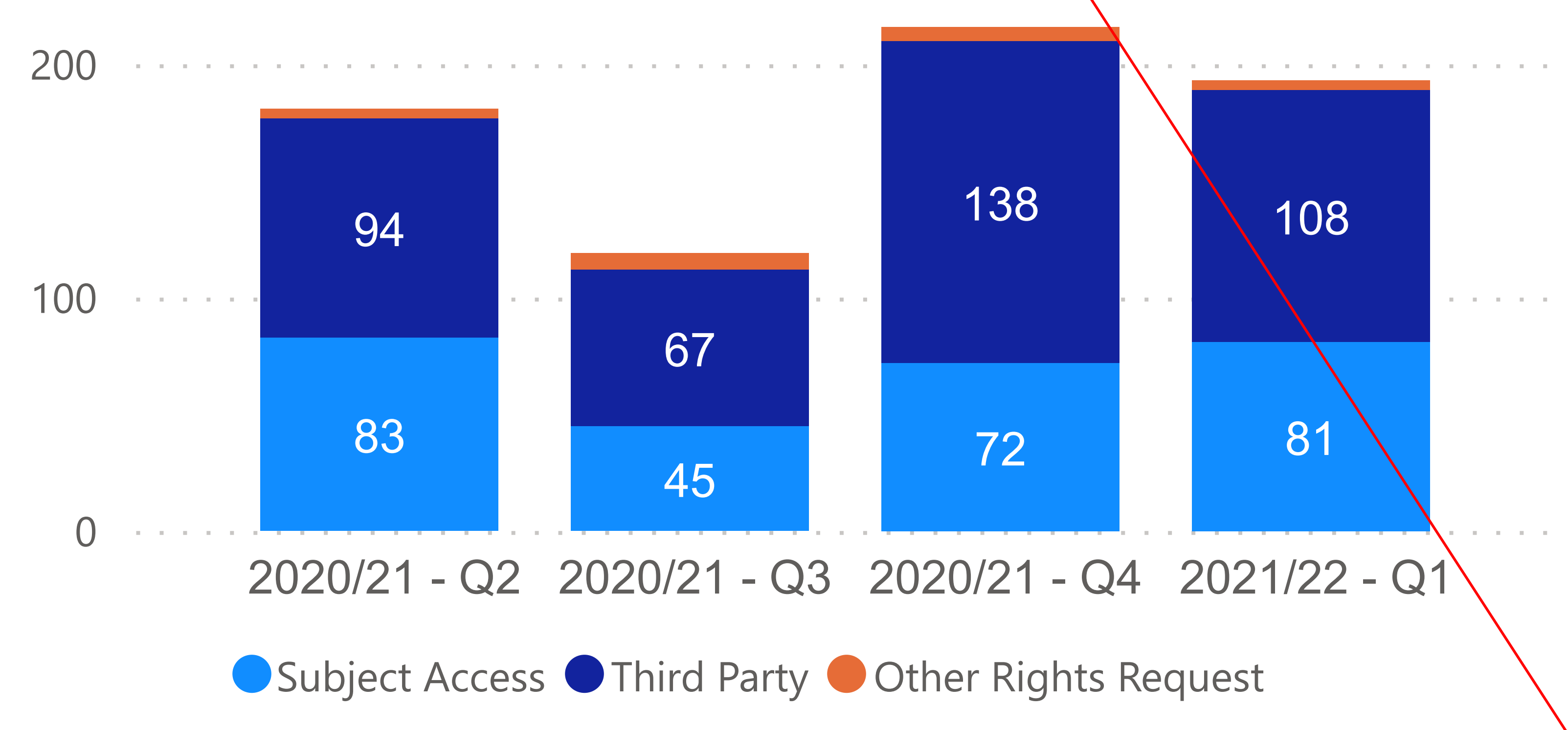


Fig 3: Corporate compliance with timescales for requests

Type of Request ▼	12 months to June 2021	12 months to June 2020
Subject Access Requests	75%	72%
Other Data Protection Rights Requests	88%	93%

Commentary on compliance

Only 21% of complex requests due in the financial year were completed within three months. Unfortunately, due to the complexity and specialism required to deal with such requests, it is challenging to consistently meet response deadlines. A specialist multi-skilled team is being recruited to within Customer Services to focus on these requests.

Data Protection Rights Requests

Data protection law gives people certain rights about their data, including the right to access their data.

Third Party Requests

Other organisations (for example, Police Scotland, or the Care Inspectorate) can also request a customer's personal data under certain circumstances.

Other Rights Requests

In certain circumstances individuals have other rights around their data: including the right to object, to erasure, to restrict processing and to data portability.

Commentary on number of requests

In the last 12 months there has been an increase in Subject Access Requests and other rights requests. There has been a decrease in reported Third Party Requests.

Timescales for responding

The statutory timescale for responding to data protection requests is between 30 and 90 days, depending on the complexity of the information being requested.

There is no statutory timescale for responding to third party requests for personal data.

2.2 Data Protection Breaches

Fig 4: Annual number of reported data breaches

Breaches	12 months to June 2021	12 months to June 2020
Data Protection Breaches	183	113
Near Misses	33	17
Reports to the ICO	6	2

Data Protection Breaches

All information security incidents should be reported. The action taken will depend on the nature of the incident or breach. Incidents will either be classified as:

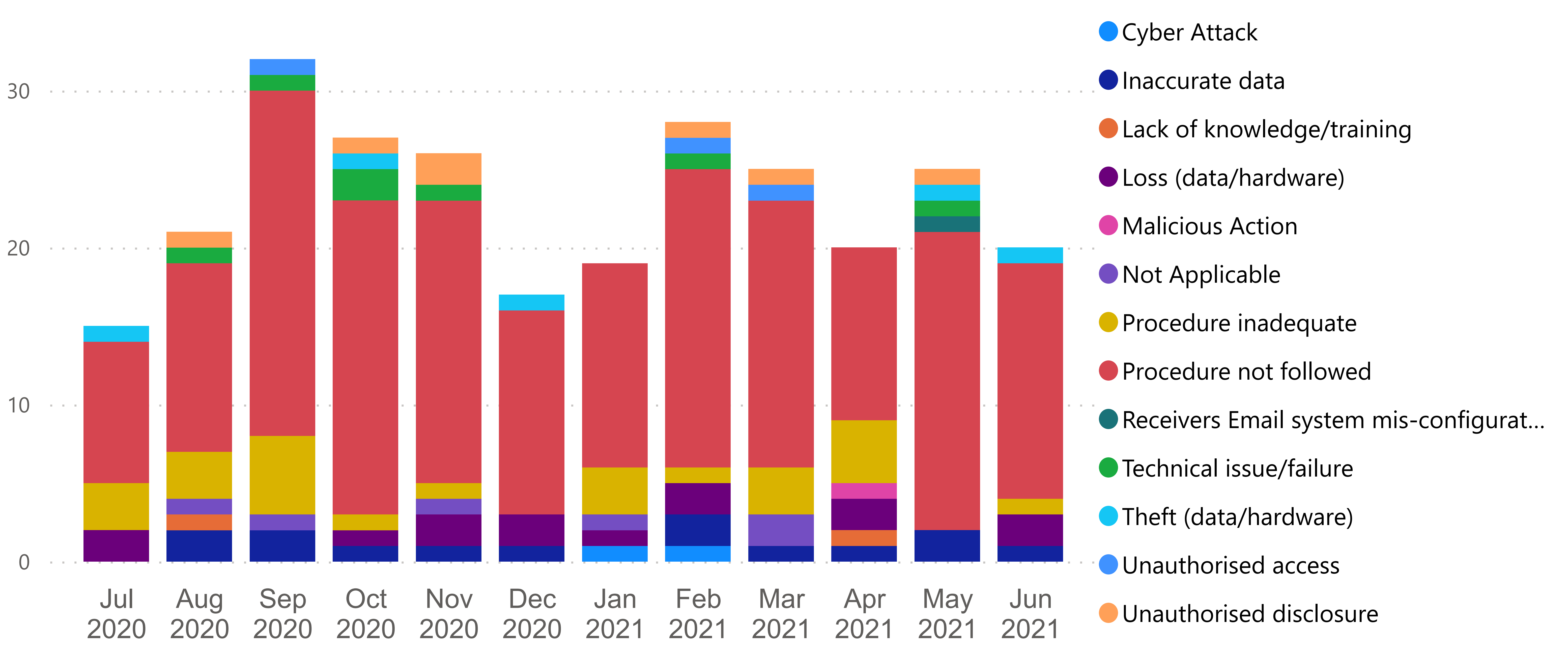
- A data protection breach
- Not a data protection breach
- Not a data protection breach but a near miss

Where a breach is likely to pose a risk to the rights and freedoms of affected individuals then the Council must also notify the Information Commissioner's Office (ICO).

Commentary on number and type of breaches

There has been an increase in reported data protection breaches this year. The figures indicate that there is a strong organisational awareness of what constitutes a breach and how to report one. The number of reported breaches remains consistent with comparable organisations.

Figure 5: Breaches by root cause in 12 months to end of June 2021



ICO Reported Breaches

There has been an increase in the number of breaches reported to the ICO in this reporting period.

The breaches which the Council has reported to the ICO in this period have been closed with no further action being taken.

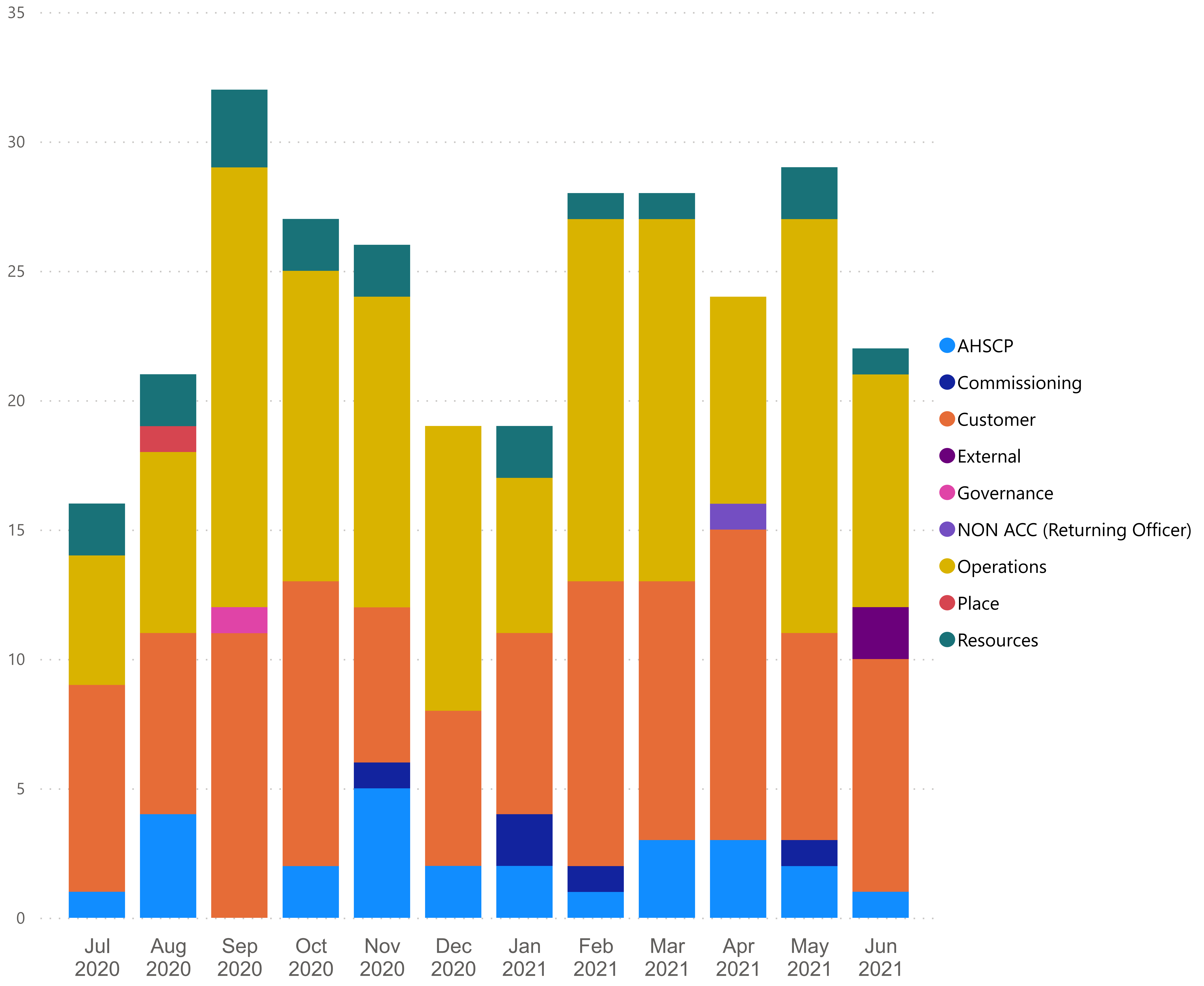
Root causes and interventions

Non-compliance with Council procedures is the main root cause of incidents in this reporting period.

Appropriate action to strengthen compliance with procedures are always identified as part of the incident handling process to ensure that controls are strengthened and to reduce the likelihood of recurrence.

2.2 Data Protection Breaches (cont'd)

Figure 6: Breaches by Function in 12 month to end June 2021



Incident and Breach Improvements

In addition to taking appropriate actions as a result of individual incidents and breaches, the Council undertakes regular monitoring of incident and breach data to identify appropriate additional actions we can take to strengthen controls. These actions are progressed through channels including the Information Governance Group, data forums led by Chief Officers, and the Council Risk Monitoring Framework.

2.3 FOISA and EIR Information Requests

FOISA and the EIRs in brief

The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIR) give anyone the right to request information held by the Council, subject to certain exceptions.

Timescales for responding

The Council must respond to any request we receive within 20 working days.

Fig 7: Annual number of requests received in the period

Number of requests received	12 months to June 2021	12 months to June 2020
Number of FOISA Requests	950	1021
Number of EIR Requests	316	456

Commentary on requests received

There has been a small decline in recorded requests, likely related to the Covid-19 pandemic.

Fig 8: Request numbers in the last 12 months

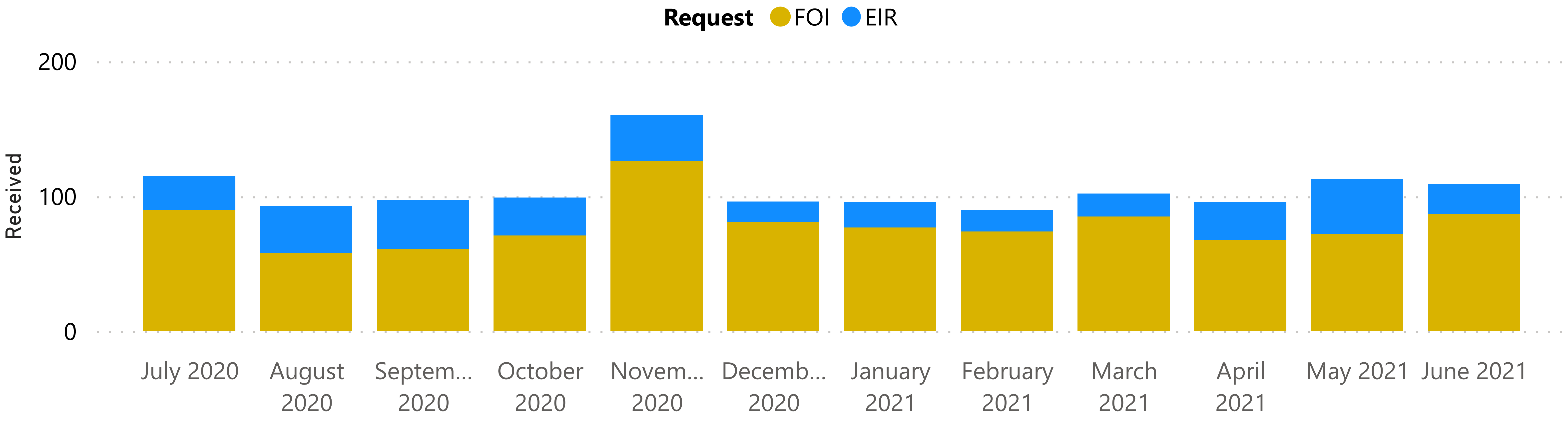


Fig 9: Compliance with timescales in the period

Number of requests received	12 months to June 2021	12 months to June 2020
Number of FOISA Requests	74%	80%
Number of EIR Requests	71%	83%

Commentary on compliance

Compliance for FOI requests has fallen. This is primarily due to the Covid 19 pandemic which had an impact on resource allocation and also access to data.

2.4 FOISA and EIR Request Internal Reviews

Fig 10: Internal Reviews received by type in the period

Type of review received	12 months to June 2021	12 months to June 2020
No response received	8	6
Unhappy with response	19	24

Internal Reviews in Brief

If the Council does not provide a response to a FOISA or EIR request within 20 working days, or if the requester is unhappy with the response we have given, they can ask the Council to review it.

Where a requester is unhappy with our response, an internal review panel will decide whether or not to uphold the original response or overturn it.

Fig 11: Internal Review Panel outcomes in the period

Type of review outcome	12 months to June 2021	12 months to June 2020
Response Upheld	20	11
Response overturned or amended	6	13

Commentary on Internal Reviews

There has been an increase in overturned or amended reviews. Areas for improvement have been identified as further training and support for officers when applying exemptions and better advice and assistance to be provided at response stage.

2.5 FOISA and EIR Request Appeals

Fig 12: FOISA and EIR Appeals received and closed in the period

No. of Appeals	12 months to June 2021	12 months to June 2020
Received	3	4
Closed	3	3

Right to Appeal

Where a requester remains unhappy with a response to a FOISA or EIR request after an internal review, they have the right to appeal to the Scottish Information Commissioner for a decision.

Commentary on Appeals

The outcome from Appeals have been positive in that where an applicant has approached the Commissioner the decision has been in our favour. The need to provide further advice and assistance was identified as a learning point.

2.6 Cyber Incidents

Fig 13: Annual number of cyber incidents in the period

Incident Type	12 months to June 2021	12 months to June 2020
Internal Cyber Incident Attempts Prevented	1	0
Internal Cyber Incidents	0	1
External Cyber Incident Attempts Prevented	9,995,496	23,900,182
External Cyber Incidents	7	8

Internal Cyber Incidents

These are risks or threats to the Council's information software, infrastructure or computer network that originate from within the premises or organisation.

Commentary on Internal Cyber Incidents

There have been no internal cyber incidents in the past 12 months.

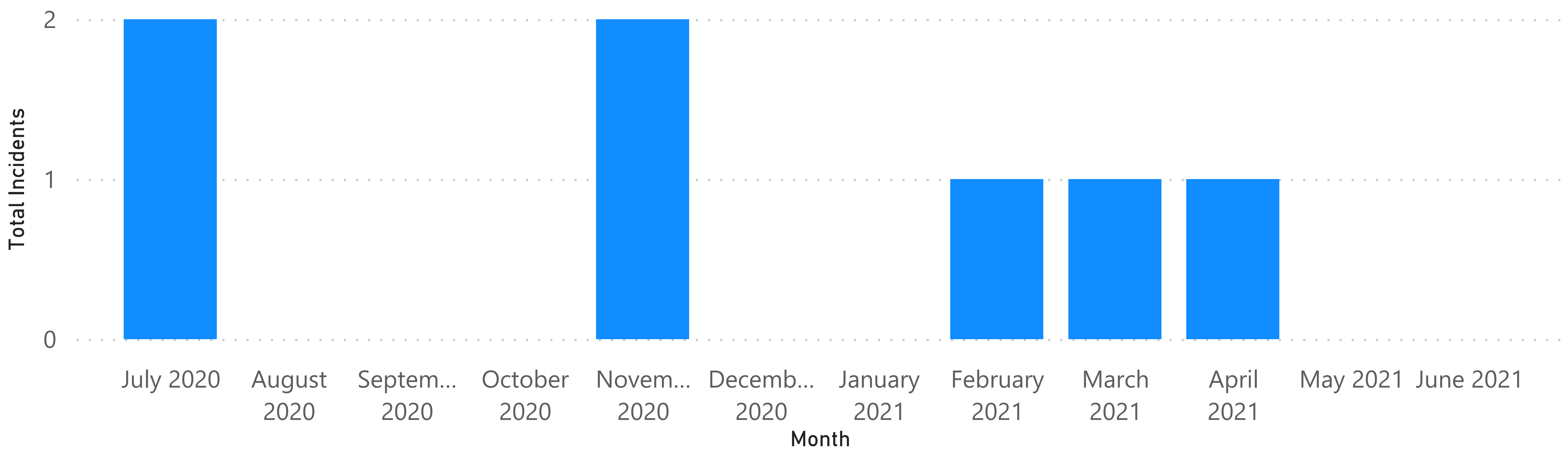
External Cyber Incidents

These are risks or threats to the Council's information software, infrastructure or computer network that originate from outside the premises or from the public (e.g. hackers).

Commentary on External Cyber Incidents

There has been a reduction in the number of external cyber incident attempts compared with the equivalent period 12 months ago. Intrusion attempts have returned to a more expected level.

Fig 15: External Cyber Incidents in the period



2.7 Lost ID Badges

Fig 13: Annual number of lost ID Badges in the period

Incident Type	12 month to June 2021	12 months to June 2020
No. lost ID badges	63	137

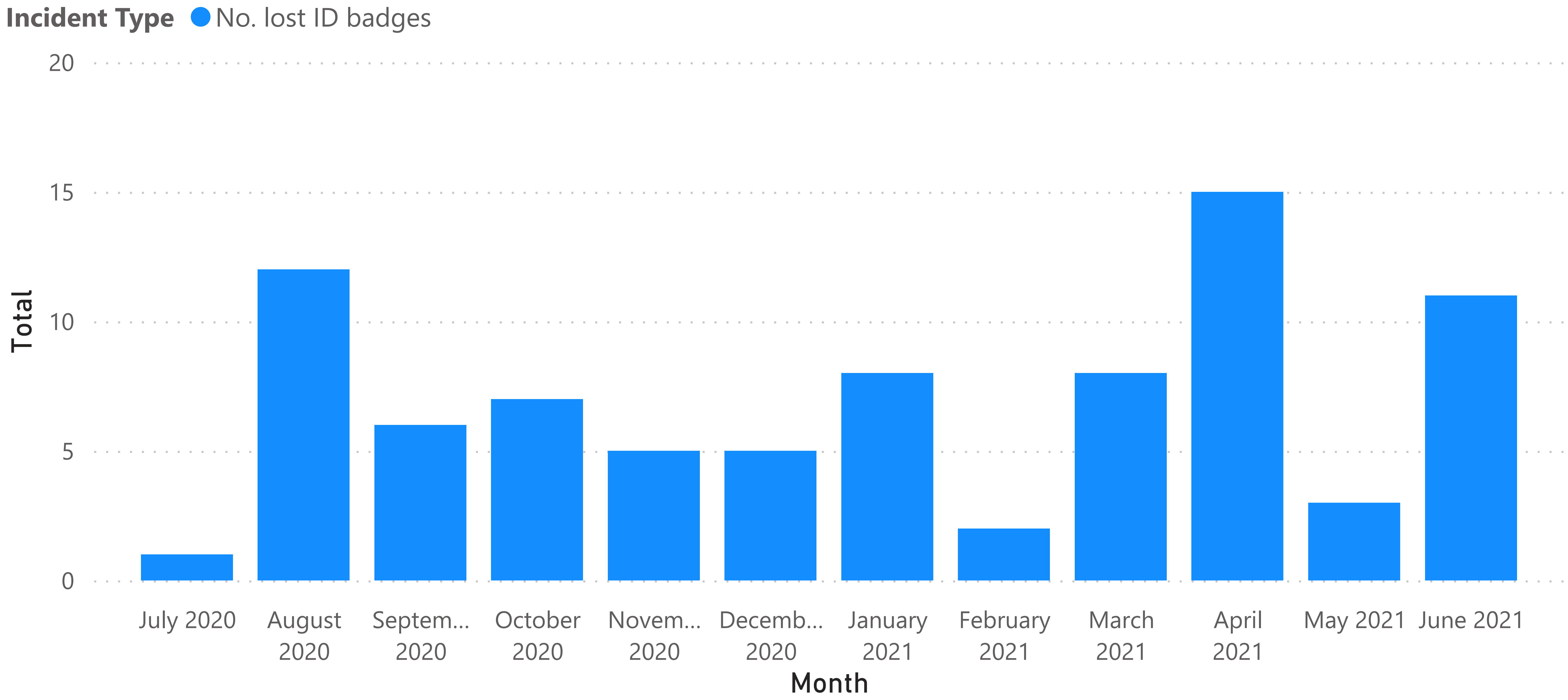
Lost ID Badges

These are tangible and material risks or threats to the Council's information assets that originate from within the premises or organisation.

Commentary on Lost ID Badges

There has been reduction in the number of lost ID badges in the past 12 months. Lost badges are deactivated following notification. The decrease coincides with COVID-19 lockdown measures and many of our staff working from home.

Fig 14: Lost ID Badges in the period


Incident Type
● No. lost ID badges
Total
July 2020
August 2020
Septem... 2020
October 2020
Novem... 2020
Decemb... 2020
January 2021
February 2021
March 2021
April 2021
May 2021
June 2021
Month