

Information Commissioner – induction briefing

Topic: ICO relationship management with key UK operational stakeholders – NCSC and LEA's.

Commissioned by: James Dipple-Johnstone.

Priority: High – to be completed and prepared for Commissioner Edwards arrival on 4 January 2021. The briefing is part of the Commissioner's induction briefing.

Owner: James Dipple-Johnstone/Steve Eckersley.

Briefing aim: To brief the Commissioner about one of the most successful and impactful relationships with a group of key law enforcement partners in the cyber security arena. The briefing will provide the Commissioner with a strong insight into the strategic value of the relationships in the context of protecting UK citizens and the UK CNI from harm and help prepare him for initial meetings with the NCSC CEO and Ministers.

List of Annexes:

Annex 1 – CYBER SECURITY DATA BREACH INCIDENT MONTHLY STATISTICS – NOVEMBER 2021

Annex 2 – Briefing for the CRO – October 2021

Background.

The National Cyber Security Centre (NCSC) is the UK's designated National Computer Emergency Incident Response team (CSIRT) and has specific responsibilities in cyber protection for the UK and its economy. The NCSC is probably the main and most important and closest ally for the ICO in the cyber security arena. Its operating centre is in London.

The NCSC is part of GCHQ and was created in October 2016. As the UK's CSIRT it has responsibility for protecting the UK's CNI. This is particularly relevant under The Security of Network & Information Systems Regulations (NIS), introduced on 10 May 2018. The NIS Regulations provide legal measures to boost the level of security (both cyber &

physical resilience) of network and information systems for the provision of essential services and digital services. The NIS Regulations came into force on 10 May 2018, you can read the regulations [here](#).

The NIS Regulations provides legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services).

The ICO is the Competent Authority for Relevant Digital Service Providers - online marketplaces, online search engines and cloud computing services. Presently, there are around 140 RDSP's registered in the UK. However, recent work as part on an ongoing ICO NIS Cyber Assessment project strongly indicates that there are probably c.1100 RDSP's falling into scope of the NIS Regulations.

The NCSC's mission statement is:

Helping to make the UK the safest place to live and work online.

We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

More specifically, the NCSC:

understands cyber security, and distils this knowledge into practical guidance that we make available to all

responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK

uses industry and academic expertise to nurture the UK's cyber security capability

reduces risks to the UK by securing public and private sector networks

<https://www.ncsc.gov.uk/section/about-ncsc/incident-management>

Graeme Biggar CBE was appointed Director General of the National Crime Agency (NCA) in October 2021, having joined the NCA as the Director

General of the National Economic Crime Centre (NECC) in March 2019. Commissioner Denham had not met Graeme. Here is a link to his profile: <https://www.nationalcrimeagency.gov.uk/who-we-are/our-leadership/senior-leader-biographies/director-general-graeme-biggar>

The National Crime Agency established the National Cyber Crime Unit (NCCU) to help combat the growing cyber-crime threat in the UK - responding to the most critical cyber incidents as well as pursuing longer-term activity against cyber criminals and helping to shut down the services on which they depend. The National Economic Crime Centre (NECC) was established a few years ago.

Since its initial establishment the NCCU has developed a UK network via its Regional Organised Crime Units (ROCU's), including UK Police forces and international law enforcement agencies. The NCA has published a number of cyber threat assessments and the most recent publication can be found here: [_pdf The cyber threat to UK business 2017/18 \(1.51 MB\)](#)

The ICO has a strong tactical relationship with the NCA/NCCU and this is most prominent at the point of cyber incident response and coordination between the ICO, NCSC, NCA and other sector regulators and cross Whitehall departments. The NCA/NCCU has a similar role to the NCSC in supporting impacted organisations subjected to cyber attacks. However, unlike the NCSC, the agency has investigative and enforcement/prosecution powers.

Section 31



These relationships are a positive way of boosting capacity and capability through secondments and analysis as we continue to build our capability in the cyber arena.

Relationship overview.


The relationship enjoyed with the NCSC has been developed over the past 5 years. The two agencies agreed an operating principles arrangement, similar to an MoU, developed through expertise and our experiences and insight gained from live operations and investigations, live exercises, policy and guidance development and publications.

The respective new and emerging technologies present genuine and potentially damaging opportunities for hostile state actors and Organised Crime Groups posing substantial risks to the UK's CNI and UK citizens. We share common interests with the NCSC and worked together in preparation for and response to threats emerging [REDACTED]

As we take on competence for some larger technology platforms following the UK's withdrawal from the EU, we are seeing notable increases in the complexity and challenge to our work investigating cyber security incidents and breaches. At the same time, the supply chain risks presented by the increasing move to cloud based services (and the vulnerabilities around CNI and complex international data transfer arrangements that go with them intersects both our NIS and GDPR remits engaging both the National Cyber Security Strategy development and the NCSC Strategic Threat Assessment mean the technical capacity and capability of both agencies is in high demand like never before.

Such is the level of trust between the two agencies, the ICO has established a unique relationship with the NCSC in the context of the 5Eyes intelligence community. The NCSC is considered a highly valuable strategic partner and our relationship elevates the ICO positively to a position of greater influence and impact across the regulated community, UK economy and government. The NCSC participates in a number of cross-Whitehall cyber related groups which, currently, the ICO does not participate in mainly because of our regulatory remit and need to be independent of the process.

The ICO has learned quickly and effectively from its incident response and investigations experience and we have developed a strong strategic and tactical relationship with the NCSC. For example, on receipt of a personal data breach notification under the GDPR or network security notification under NIS the ICO may contact the NCSC operational team directly to discuss the incident response, comms lines, etc and visa versa. If the breach notification involves financial data the NCSC and [REDACTED]



The ICO has also collaborated successfully with the NCSC to develop and implement policy and guidance, for example the 'Cyber Essentials' programme. We are currently working with the NCSC to share our understanding of strategic threats concerning MSP's, smart cities, Adtech and a Home Office Project – Cyber Duty to Protect and more recently development of the NIS Cyber Assessments Framework (CAF) for RDSP's.

The NCSC operates a number of important and influential schemes, including the Cyber Incident Response (CIR) scheme to certify companies who can help organisations who have been the victim of a significant cyber attack and the Cyber Security Information Sharing Partnership (CiSP). Under the CIR scheme there are seven CIR registered companies offering cyber incident response support to impacted organisations. The ICO regularly participates in the quarterly NCSC/CIR workshops aimed at improving services.

The CISP is a joint industry and government initiative set up to allow UK organisations to share cyber threat information in a secure and confidential environment. As a regulator, the ICO is not permitted to join the scheme so given the penetration of the NCSC within the regulated community the ICO has relied on the NCSC to help land key messages. For example, the availability and utility of the ICO's GDPR cyber-security guidance.


Strategically, the ICO hold CEO bi-lateral meetings with the NCSC every quarter. We also participate in multi-agency quarterly 'business breakfast' chaired by the NCSC CEO.

The briefing for the most recent executive meeting with the NCSC is attached at annex A. The ICO is also chair of a 'Quadrilateral' meeting held quarterly involving senior representatives of the NCSC, DCMS and National Crime Agency/National Cyber Crime Unit (NCA/NCCU). The Home Office recently joined the meeting given the proximity of their cyber related project work. The main purpose of this meeting is to develop policy and surface shared understanding of cyber threats and opportunities.

Section 31



At tactical level, the ICO is chair of the 

 The purpose of this meeting is to share information re current and emerging trends and threats, such as Ransomware and to develop an effective coordinated response.

The ICO and NCSC, together with the National Crime Agency (NCA) and National Cyber Crime Unit (NCCU) have participated in joint-exercises aimed at developing 'play books' to help manage incident response and confliction between agencies, which has proved invaluable. The play book has been a key feature in helping improve the UK's incident response and investigation of cyber security and cyber crime

Section 31



Key considerations for the Commissioner includes establishing and developing high-level and strategic partnership with the NCSC and cross-Whitehall groups and the UK Intelligence Community (UKIC) and the NCA/NCCU to create pathways for additional and new impact and influence opportunities and to help shape and support the current and developing strategic and tactical relationships as the ICO's ambition around cyber security becomes clearer.

The ICO leads for the various meetings are as follows:

NCSC CEO Breakfasts and bi-monthly meetings – James Dipple - Johnstone.

Quadrilateral – Steve Eckersley, Director of Investigations

██████ – Sally Baker, Group Manager, Cyber Incident Response and Investigations Team.

NCA bi-annual - James Dipple – Johnstone

NCA quarterly - Steve Eckersley.

Author : Steve Eckersley

Date of briefing : 8 December 2021

Reference no: [will be provided to you in commissioning request]

Prepared for: John Edwards, Information Commissioner

Consultees: Hazel Padmore

Reviewed/cleared by:

For Commissioner use only - Follow-up required:

[A field for the Commissioner to use to include any initial thoughts on further follow up if required.]

ANNEX 1 — CYBER SECURITY DATA BREACH INCIDENT MONTHLY STATISTICS — NOVEMBER 2021.

Briefing for Chief Regulatory Officer

Cyber Update

Date: 12 October 2021
External publication: No
Internal publication: No
For decision: No
Security marking: Official sensitive.

1.0 Reason for report

This briefing has been prepared following a request from James Dipple-Johnstone, Chief Regulatory Officer, in advance of his meeting with Eleanor Fairford from NCSC on 15 October 2021.

2.0 Update on Cyber Incident Reports

In August we received 141 cyber reports, a significant reduction from the previous month during which we received 239 reports. Of these, 73 were triaged by CIRIT and 68 were low level phishing reports that were dealt with by PDB. Similar declines in reporting during August have been observed in previous years. Although a decline in reporting can be seen in all sectors, the most significant decline occurred in the education and childcare sector.

Ransomware reports decreased from 90 in July to 25 during August. However ransomware and unauthorised continue to represent the majority of the incidents that are triaged by the CIRIT team (67%). Data on reports received since the start of this financial year shows that 31% of the reports made by the Legal sector have been in relation to malware attacks. This is a much higher percentage than any other sector.

3.0 Update on Cyber Related Activity

3.1 – NIS – Development of an Assurance Oversight Model

The ICO continues to work closely with the NCSC in relation to its development of an assurance oversight model for RDSPs. In addition, our external partner, Gartner, has now been appointed and we have commenced discussions with a small number of RDSPs (c.40) with whom we wish to engage in relation to development and pilot of potential models for the assurance model. We anticipate that the development of the proposed model will be concluded during November, with feedback being sought from parties over the following months.

3.2 – NIS Register

Gartner has also been appointed to provide us with a comprehensive risk prioritised register of organisations that fall within the definition of a digital service provider under NIS. This will enable us to undertake a review of our existing register, identifying organisations that have yet to register with us under NIS. It will also enable us to get a better understanding of the risk profile of the organisations to support delivery of future supervisory activity.

3.3 – Amendments to the NIS Regulations – thresholds for reporting

We continue to engage with DCMS with regard to amendments to the NIS Regulations. With regard to the proposed amendments to the thresholds for reporting, DCMS have secured ministerial approval to proceed with proposals that would provide the ICO with the power to set reporting thresholds in guidance. DCMS ran a public consultation in relation to this amendment during August. We have subsequently launched our own consultation to obtain views on the threshold model that would be set out in guidance. We sought an opinion from NCSC on the proposed options to be included in the consultation prior to its publication.

3.4 – Regulation of cloud service providers

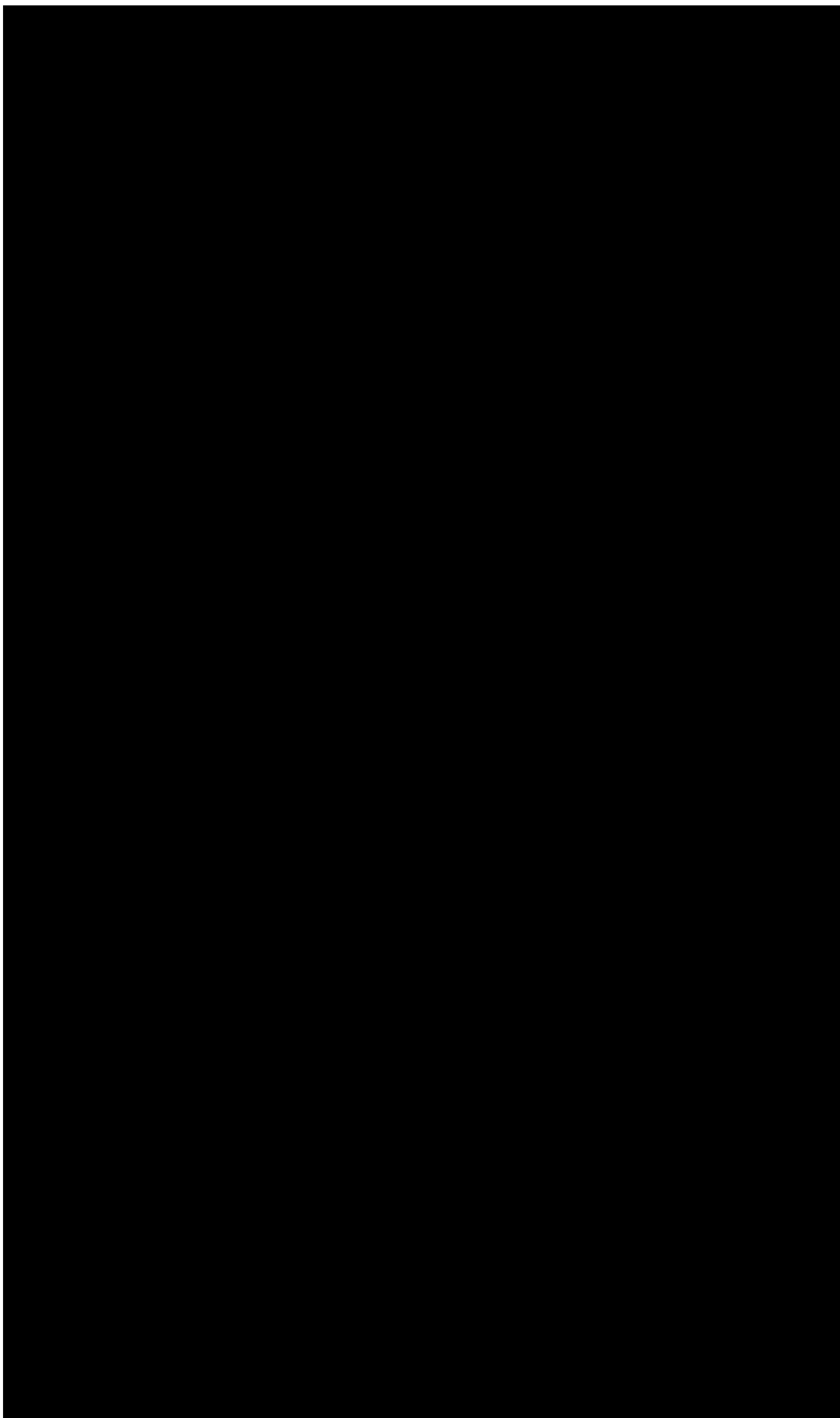
Following the policy proposals from DCMS [REDACTED] there has been continued engagement between NCSC, ICO, DCMS and other departments on how this proposal might be approached, particularly with reference to the definitions to be engaged and thresholds for designation. Both organisations attended a workshop with DCMS on 14 September 2021. A further session was held on 28 September 2021 between the ICO and NCSC. DCMS has subsequently invited competent authorities and NCSC to provide feedback on the proposed public consultation in relation to this amendment [Section 31] [REDACTED] It is intended that the public consultation will be launched in November 2021.

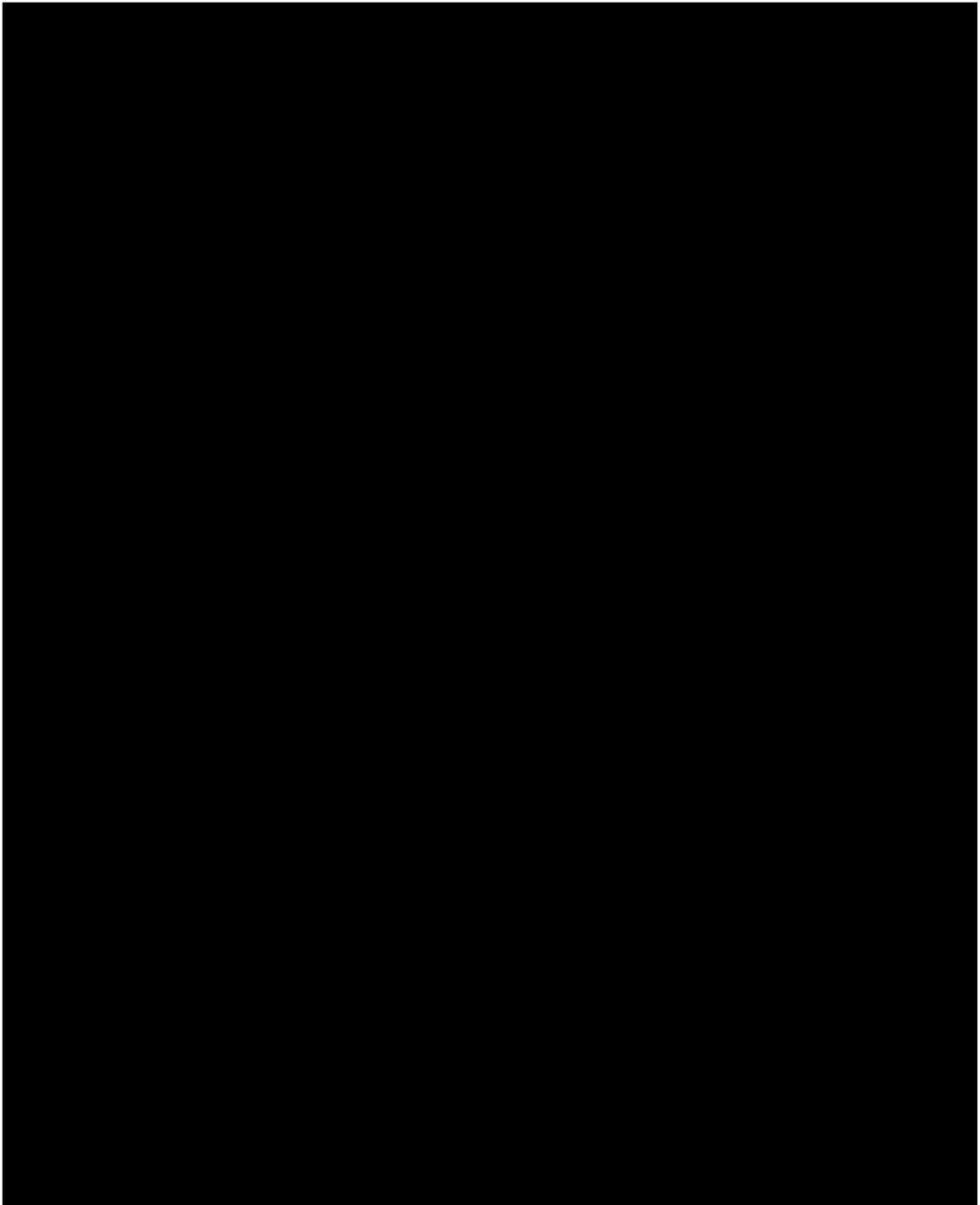
4.0 Update on Cyber Investigations

Section 31



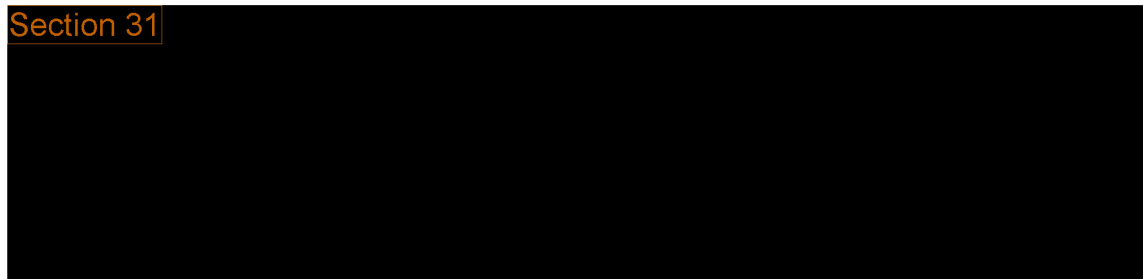
- Official Sensitive-

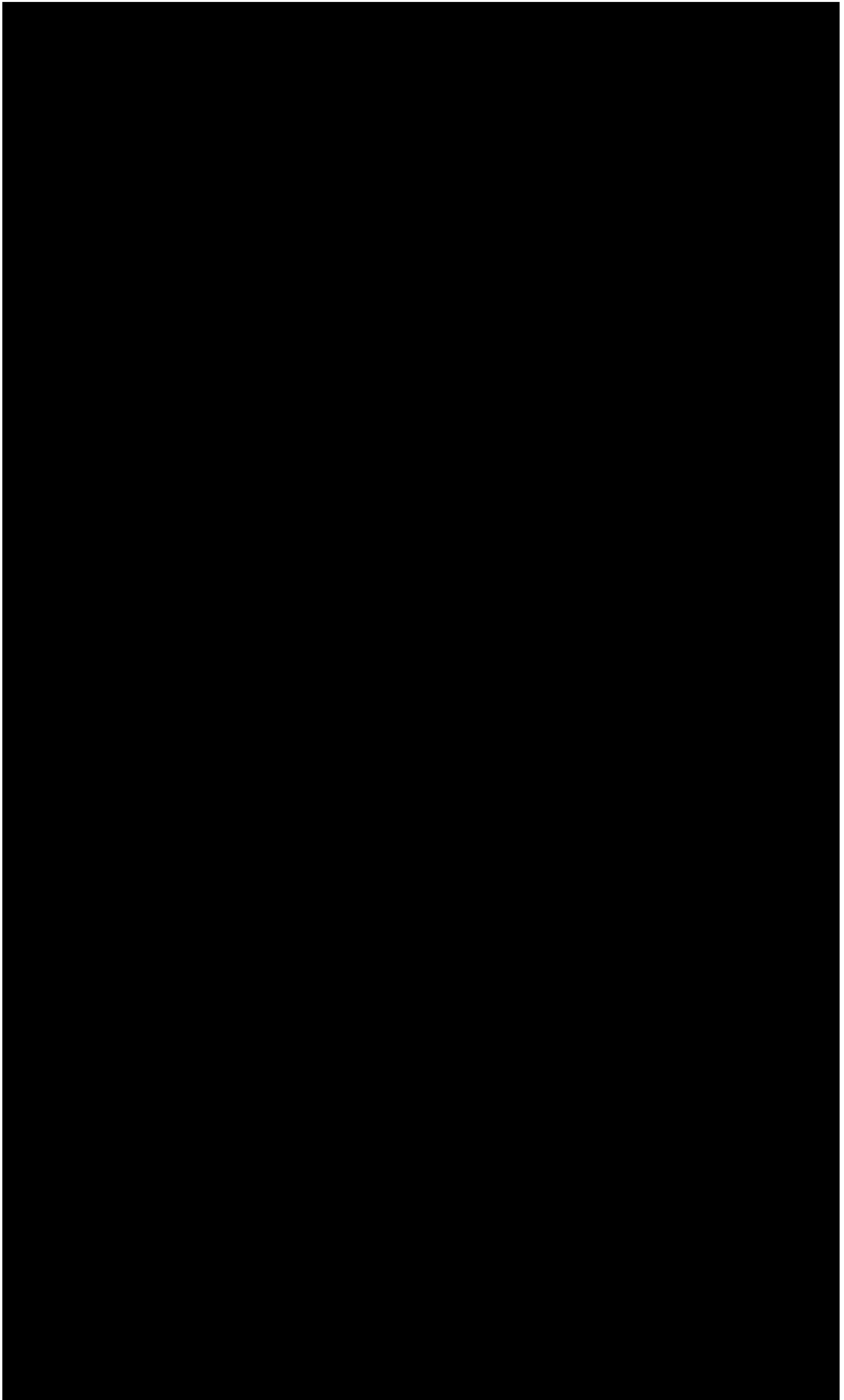




Recent potential significant cases not currently on the case tracker:

Section 31

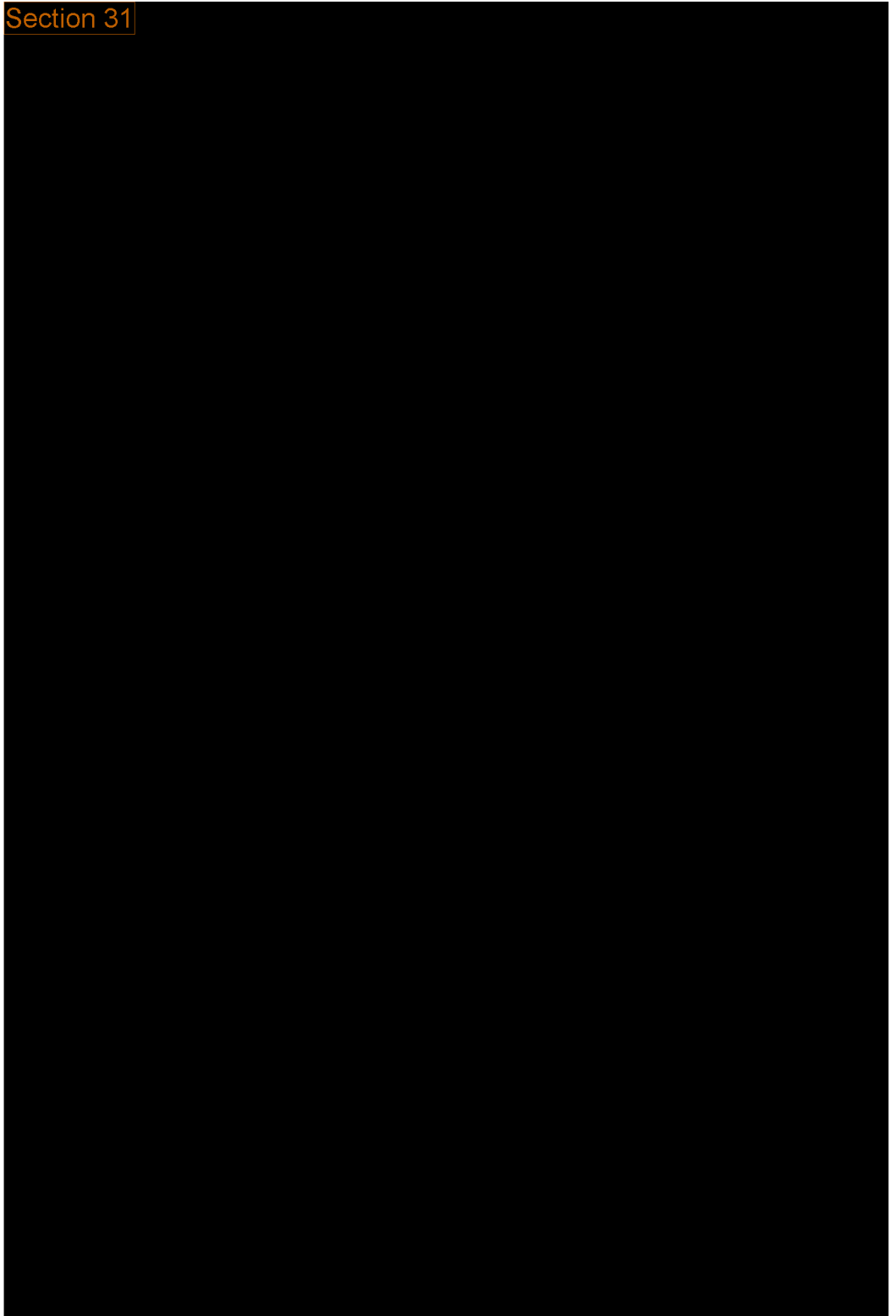


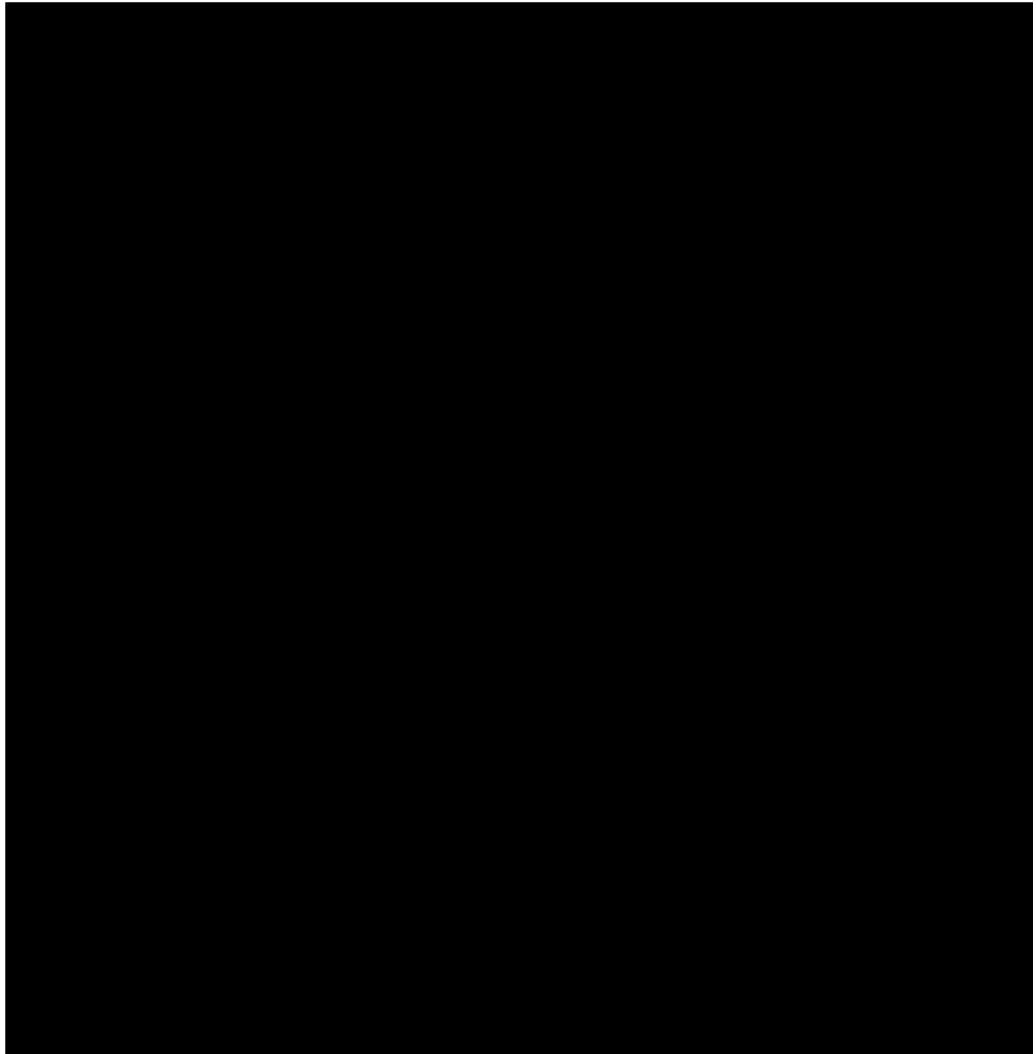




Cases Progressing to Recommendation for Proposed Regulatory Action in Q2 (2021).

Section 31

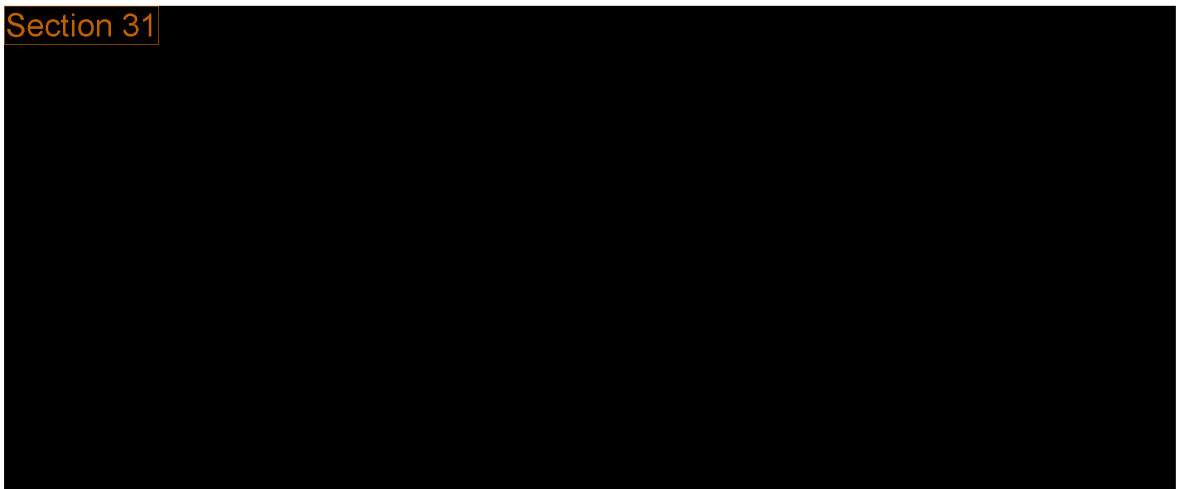


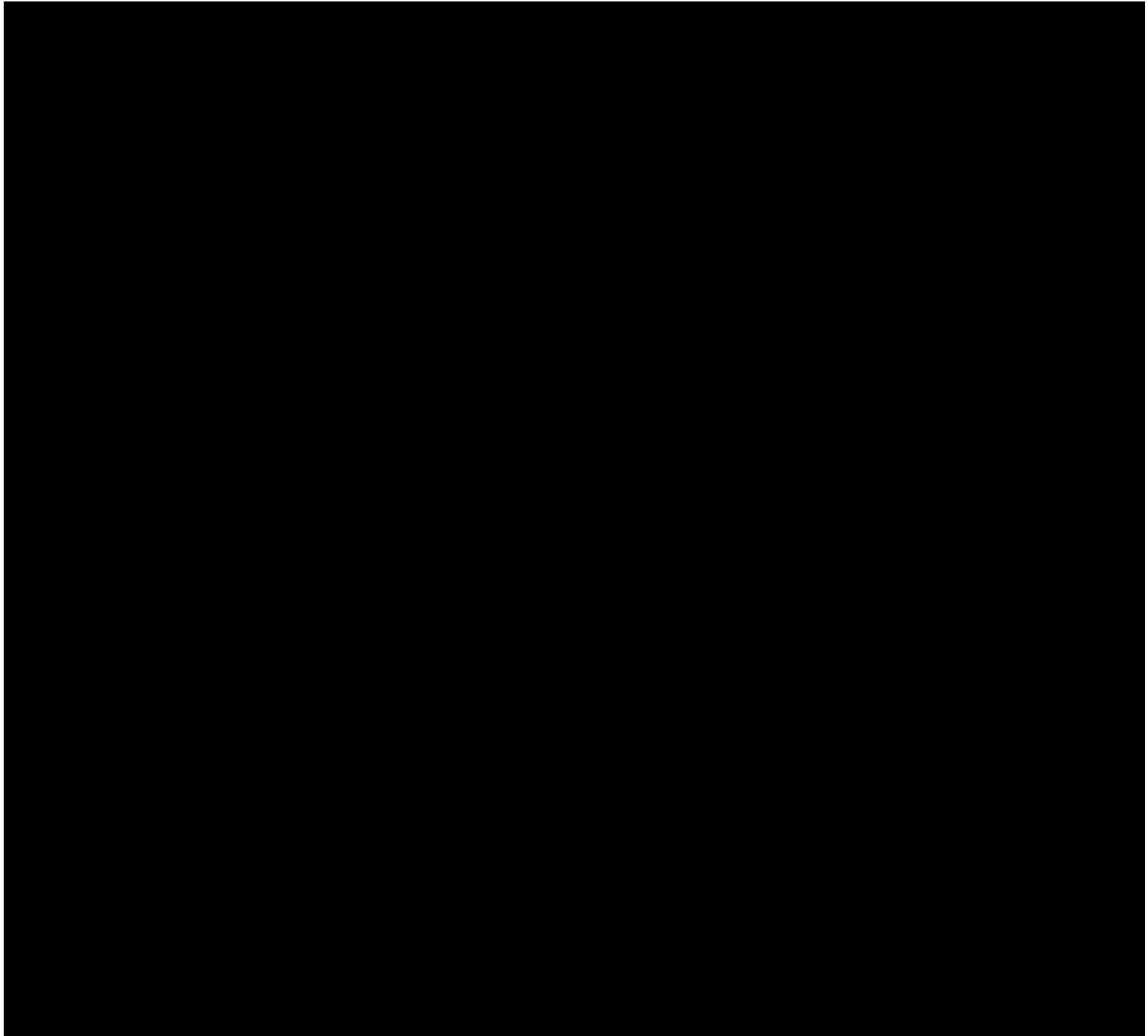


Incidents

CIRIT have responded to the following potentially significant incidents over recent weeks:

Section 31





[5.0 Communications considerations](#): None at the present time.

[6.0. Equality, diversity and inclusion considerations](#): There are no equality and diversity considerations in relation to this report.

[7.0. Alignment with values](#): Ambitious – shows the volume and scope of incidents and investigations being conducted by CIRIT.

[8.0. Link to the Information Rights Strategic Plan](#): Goal 5

[9.0. Impact on Risks and Opportunity Register](#): n/a

[10.0. Author](#): Hazel Padmore (HoI)

[11.0. Approved by](#): Steve Eckersley, Director Investigations

This report presents the cybersecurity personal data breach notifications assessed and triaged by the ICO's Cyber Incident Response and Investigation Team (CIRIT)



Total cybersecurity incidents reported to the ICO – 185:

- 141 incidents were triaged by CIRIT
- 44 low-level phishing incidents were handled by the Personal Data Breach (PDB) team



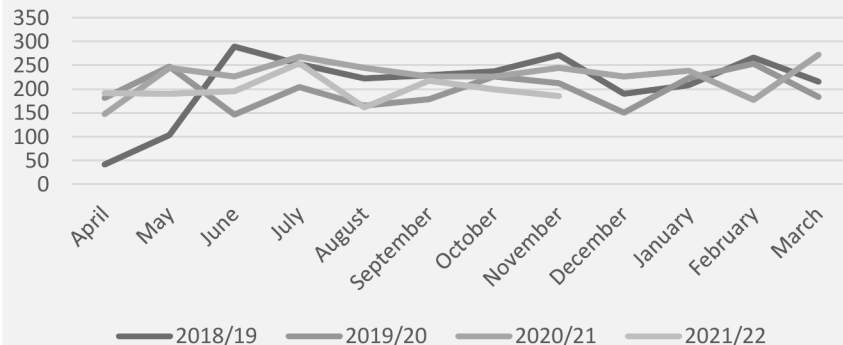
25 incidents were referred for further investigation



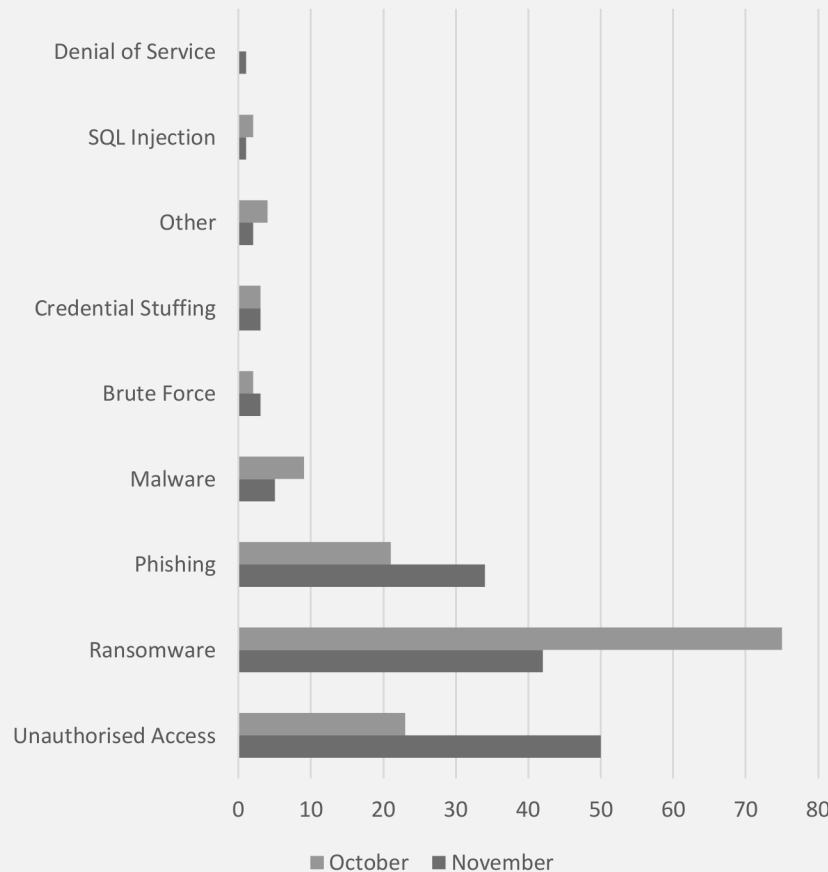
Retail and Manufacturing was the highest reporting sector

Incidents reported

2018/19, 2019/20, 2020/21 and 2021/22



CYBERSECURITY ISSUES REVIEWED BY CIRIT



Published Draft

Contacts

Incident Management

Email: Cyber Incidents Section 31

Intelligence Hub

9am-5pm (working days)

Email: [\[Redacted\]](mailto:)

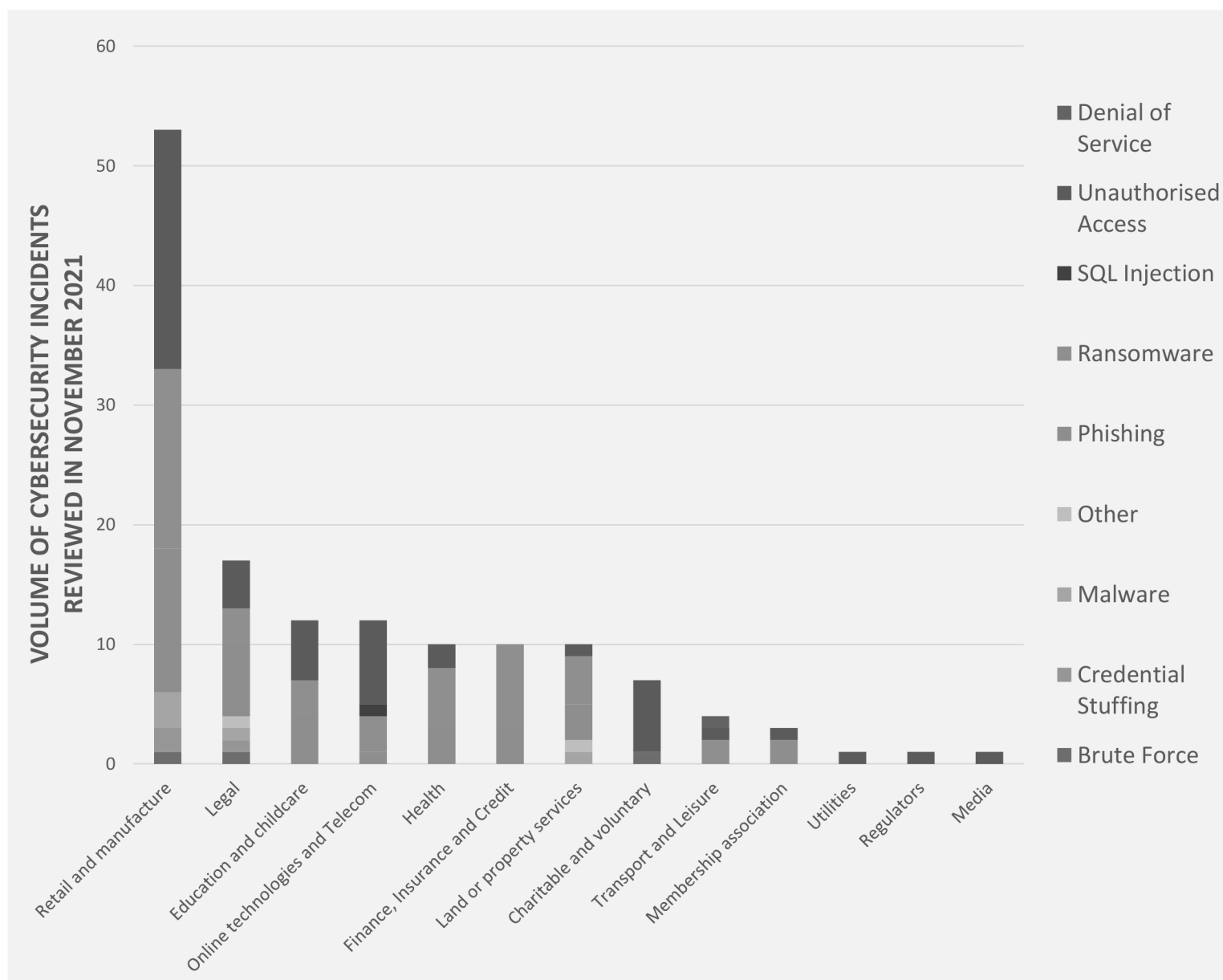
Press enquiries

08:30-17:30 (working days)

Email: pressoffice@ico.org.uk

24/7 Tel: 0303 123 9070

DATA BREACH NOTIFICATIONS REVIEWED BY THE CYBER INCIDENT RESPONSE AND INVESTIGATION TEAM IN NOVEMBER 2021



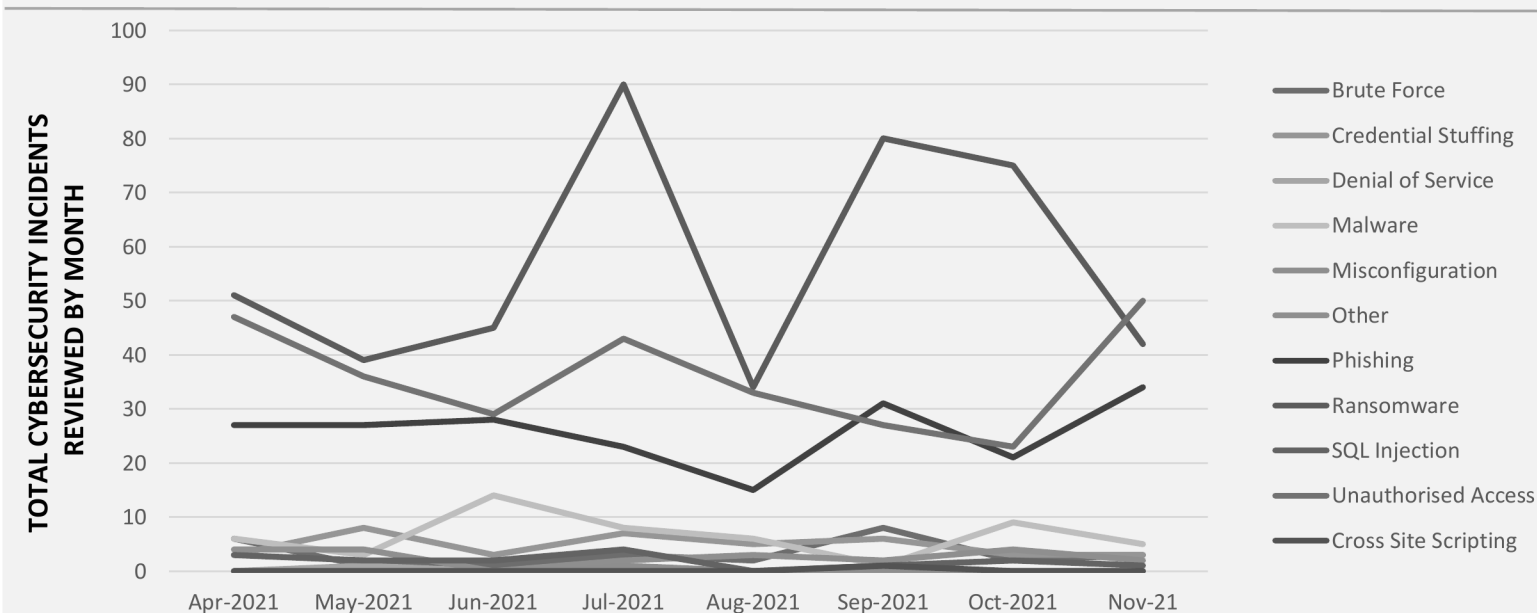
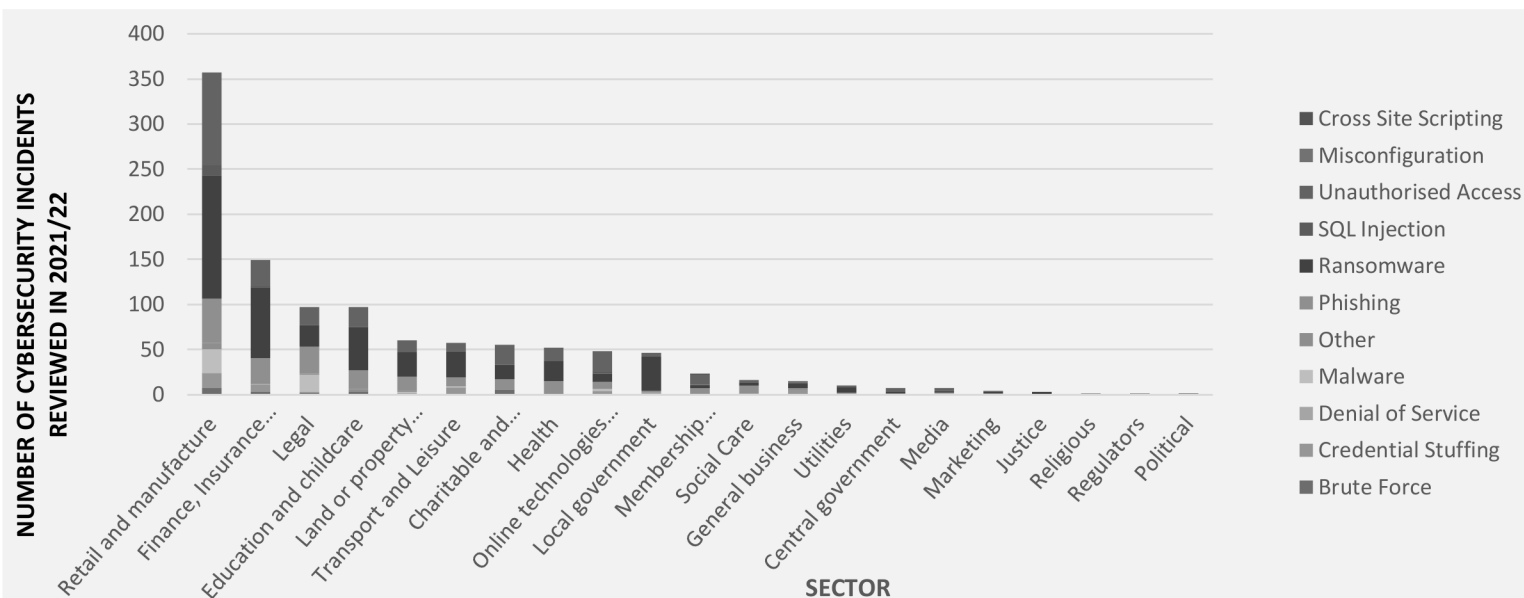
KEY OBSERVATIONS: NOVEMBER 2021

CIRIT reviewed 50 Unauthorised access incidents received in November 2021, up from 23 – a 117% increase. This is in part linked to multiple reports from data controllers affected by an Unauthorised access incident targeting a website provider.

As a result, this is the first time since April 2021 that Ransomware incidents are not the most reviewed type of incidents.

A high number of reports from the Legal sector were reviewed – 17 reports representing the second highest figure for the sector since April 2021. However, these are spread across multiple incident types and do not appear to be indicative of a specific trend.

DATA BREACH NOTIFICATIONS REVIEWED BY THE CYBER INCIDENT RESPONSE AND INVESTIGATION TEAM FY 2021/22

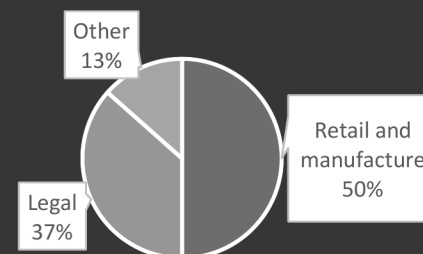


KEY OBSERVATIONS: 2021-22 financial year

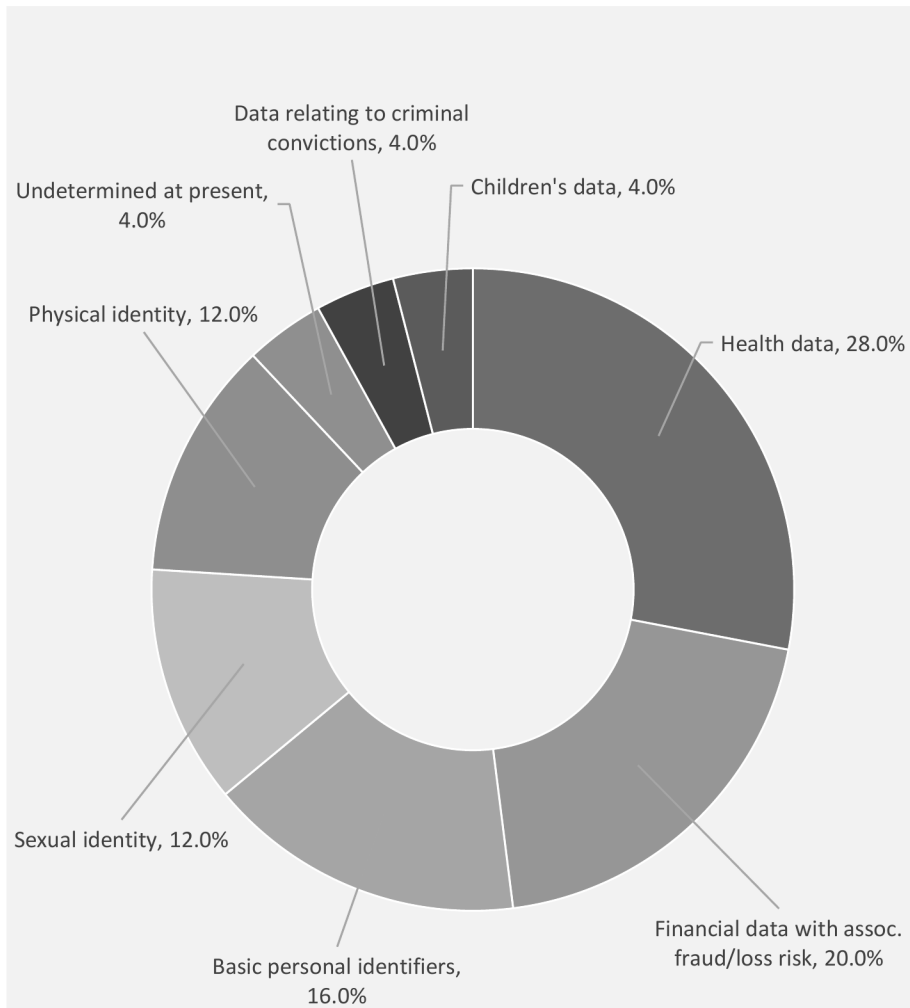
Reports of Ransomware incidents decreased by 44% in November 2021, but remained on par with levels seen between April and June 2021.

The Legal and Education and childcare sectors have now both reported 97 incidents since April 2021 and are now the third highest reporting sectors.

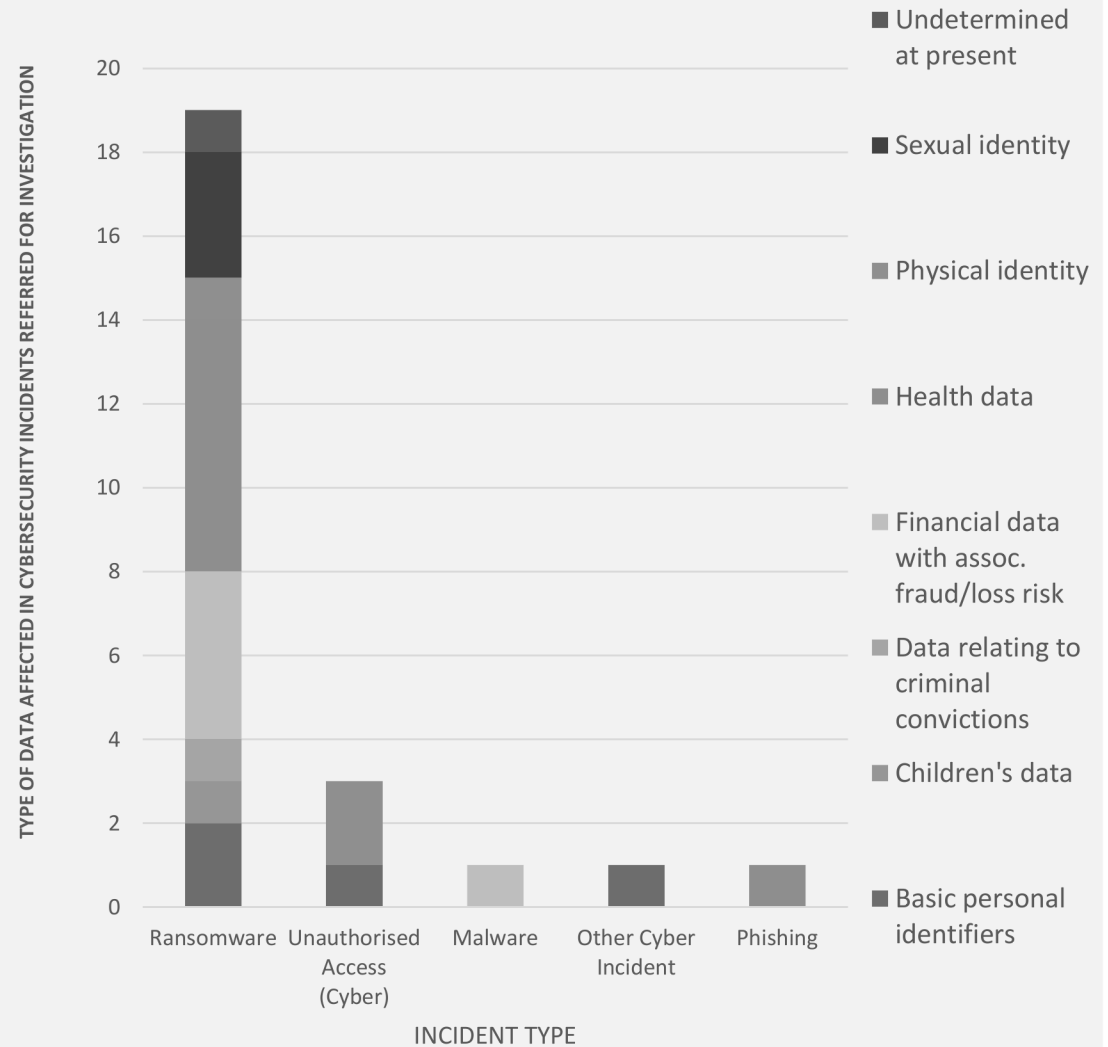
As noted in the August 2021 report, the Legal sector has reported a noticeably higher number of Malware incidents compared to other sectors (except the Retail and manufacture sector):



MOST SENSITIVE DATA AFFECTED BY CYBERSECURITY INCIDENTS REFERRED TO INVESTIGATIONS IN NOVEMBER 2021



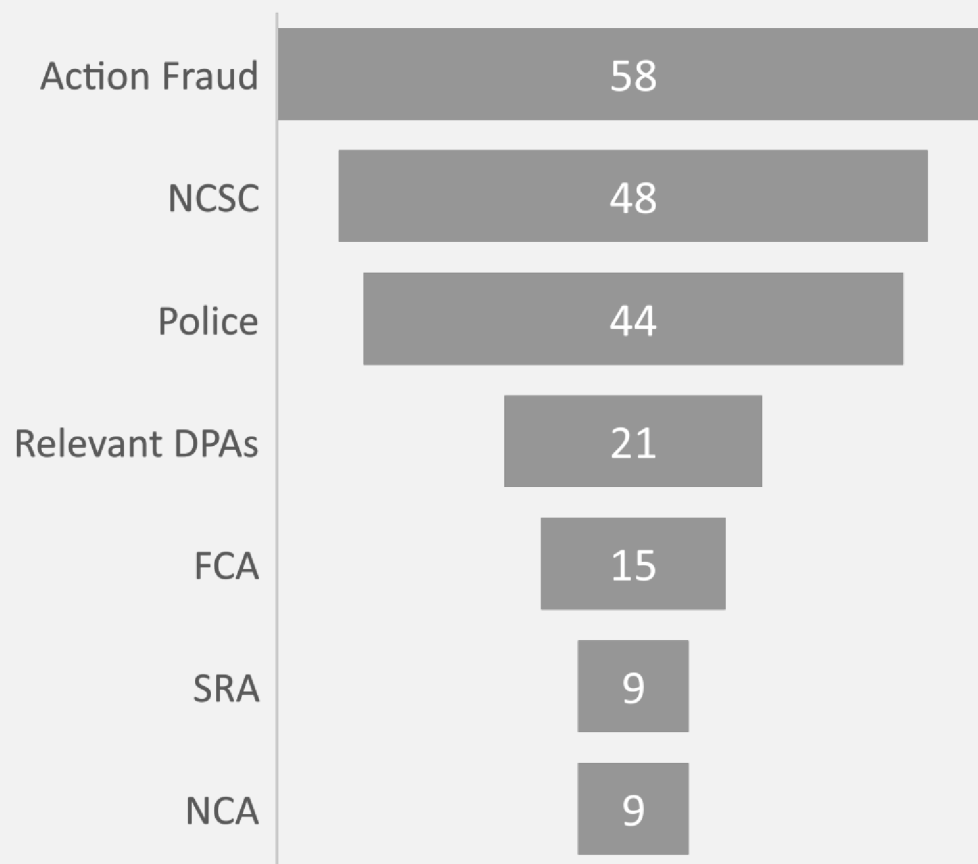
Note: The figures in these charts are based on incidents referred to Investigations in November 2021



SOURCES AND REFERRALS OF CYBERSECURITY INCIDENTS REFERRED TO INVESTIGATIONS FY 2021-22

INCIDENTS REFERRED TO OTHER AUTHORITIES

This includes referrals made directly by the data controller and referrals made by the ICO.



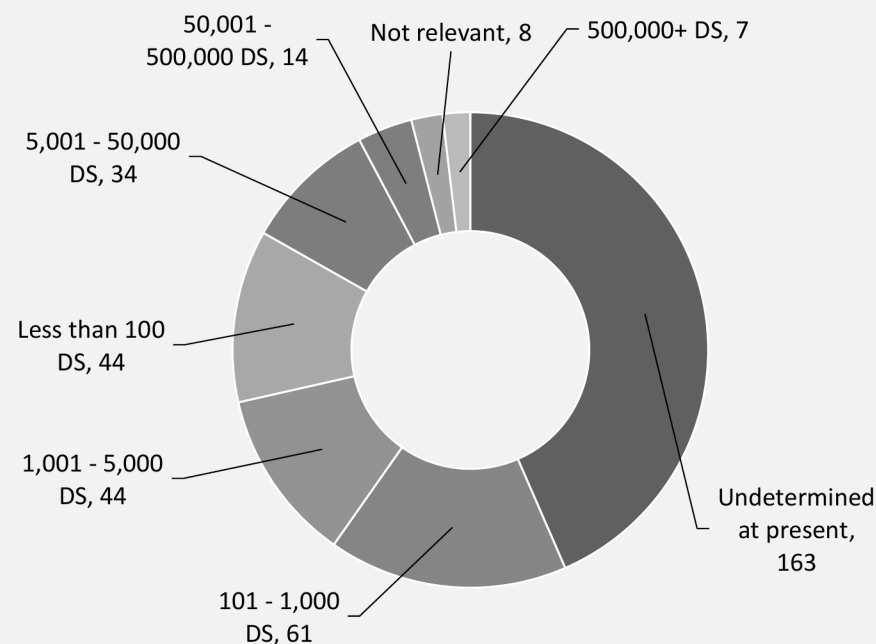
Note: The figures in these charts are based on incidents referred to Investigations in the financial year 2021/22

SOURCE OF INCIDENTS REFERRED TO INVESTIGATIONS FY 2021/22

375 reported total

367 Reported by Data Controller
3 Reported by a third party
3 Reported by Data Processor
1 Reported by Data Subject
1 Reported by the media

NUMBER OF DATA SUBJECTS AFFECTED BY CYBERSECURITY BREACHES REFERRED TO INVESTIGATIONS



Note on figures and statistics

From April 2021, the figures and dates contained in this report are based on the incidents reviewed by the Cyber Incident Response and Investigation Team (CIRIT) unless otherwise stated. Cybersecurity incidents affecting data processors may generate a high number of personal data breaches reports to the ICO from data controllers affected by the incidents. In such cases, these reports may be added retroactively to the figures contained in this report as and when they are reviewed by CIRIT.

Figures and dates prior to April 2021 are based on the incoming incidents reported to the Personal Data Breach team prior to assessment by Investigation Teams.

Data is taken as a snapshot in time from a live database. Historic data is liable to change as updates are made.

The ICO publishes quarterly data security incident trends statistics on our website. The latest report can be found at the link below;

<https://ico.org.uk/action-weve-taken/data-security-incident-trends/>