Information Governance Management

Annual Report

Senior Information Risk Owner

July 2016-
June 2017

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 first of these reports.

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

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, the Information Governance Group has established an Information Assurance Improvement Plan which will implement the required medium term assurance improvements required. The Information Assurance Improvement Plan is focussed on the following nine key assurance areas:

- Oversight & Control
- Legal & Business Requirements
- Technical & Physical Security
- Business Continuity & Disaster Recovery
- Information Sharing & Integration
- Culture, Awareness & Training
- Information Preservation
- Information for Strategic Performance Management & Transformation
- Realising Information Re-use Value

1.6 The Executive Summary at Section 2 of this report brings together the Information Governance Group's key activities from the last year; this includes activity arising from the ongoing monitoring of performance, and measures to improve assurance in the medium term.

2. Information Assurance Improvement Plan: Executive Summary of progress to June 2017

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Oversight & Control	Information Governance related monitoring and reporting fragmented across Council	IG Group developed and implemented Consolidated Quarterly Information Governance monitoring and reporting	Regular quarterly monitoring and reporting in place, with annual reporting to Audit, Risk & Scrutiny Committee	IG Group will continue to monitor and report on IG and to take appropriate remedial action as required	The Council is undertaking appropriate monitoring, and continuously improving assurance around its information and data
	Requirement for joined up approach to effect medium term information assurance improvements	IG Group developed Assurance Improvement Plan: agreed and underway	There's a joined up information assurance improvement plan underway which will implement, monitor and manage sustainable improvement to information governance across the Council	Continue to implement plan and include progress updates in quarterly Information Governance Reports	The Council is continuously improving assurance around its information and data
	Lack of corporate standards in place for data governance	Corporate Data Office established to implement corporate approach to data governance	Regular data forums in place where data quality in key systems is monitored	Develop data governance measures and standards through regular data forums	The Council has the foundational data governance in place required to implement master data management
	Requirement to raise knowledge and awareness amongst third tier managers of their Information Governance related responsibilities	IG Group developed 'Information Asset Owner' sessions and guidance for third tier managers, with sessions to run in September 2017	Clear guidance and supporting training sessions in place for third tier managers setting out their Information Governance related responsibilities	Complete sessions for third tier managers, prioritised by those who handle personal information. Use feedback to feedback from sessions to manage and improve further training or guidance required	Our Senior Managers are confident and knowledgeable about their role in the proper use and governance of the council's Information and data
	Council Information Asset register required to be updated to include information required for GDPR readiness and	Information Asset Register redesigned, and updated with additional fields developed	Information Asset Register fit to enable GDPR compliance activities	Implement a regular Information Asset Assurance programme in place through our Information Asset	The Council has assurance about the management of its information assets

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
	compliance			Owners	
Legal & Business Requirements	Council needs to be ready for changes to Data Protection law (GDPR) which are enforceable from May 2018	IG Group developed Assurance Improvement Plan includes activities required for GDPR readiness: agreed and underway	Joined up improvement plan underway which will implement the required GDPR readiness activities	Continue to implement plan and include progress updates in quarterly Information Governance Reports	The Council is preparing appropriately for changes to data protection law as part of a holistic approach to improving the management of its information and data
	Aberdeen City Licensing Board did not have Records Management Plan in accordance with requirements of Public Records (Scotland) Act 2011	Joint working to agree a consolidated and combined Records Management Plan for Aberdeen City Council & Licensing Board	Joint Aberdeen City Council & Licensing Board Records Management Plan approved by Regulator in Feb 2016	Monitor progress through the IG Group and provide formal annual updates to Regulator as requested	The Council and Licensing Board are complying with the requirements of the Public Records (Scotland) Act 2011
	Multiple corporate information and data related policies in place. Potentially confusing for staff and members	Joint working to review information and data policy. Consolidated and streamlined Information Policy developed by IG Group	Corporate Information Policy developed for consideration and approval at Finance Policy & Resources in Sept 2017	Review and update supporting procedures and guidance	Everyone understands what the Council's Information Policy is, what it means for them, and how they comply with it
	Dip in FOI compliance with statutory timescales in March 2017	FOI request media approval process reviewed and revised	FOI Compliance with timescales improved and overall compliance for the period remained high	Continue to monitor FOI compliance figures and take appropriate remedial action as required	To ensure that the Council complies with the Freedom of Information (Scotland) Act 2002
	Increase in data incidents and breaches in comparison to preceding reporting period	IG Group worked with Organisational Development & Communications to analyse underlying causes and design appropriate campaign	'Information Matters' awareness campaign designed and created to run in September 2017	Ongoing monitoring of breaches, analysis of campaign effectiveness and appropriate additional remedial actions required	The Council learns from data incidents and breaches which occur and uses evidence to inform and test appropriate remedial action
Technical &	The Council's firewall required updating to take advantage of advances in available	Next Generation Firewall has been implemented	The Council has up to date firewall protection in place	Tuning and further development of the solution to reach the best operational	The Council is keeping its cyber network protection up to date

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Physical Security	solutions			configuration	
	The Council requires to implement secure email solution for external communication	TLS and SPF implemented	Implement Secure Email Blueprint	Implement DMARK and DKIM	The Council has appropriate security of email communication and assurance for the public
Information Sharing & Integration	Information Sharing guidance and protocols required to be reviewed due to changes in data protection law which are enforceable in May 2018	Information Sharing Protocol (ISP) Register created	The Council understands its current information sharing arrangements	Review sharing arrangements and update agreements where required. Review and update, as appropriate, information sharing procedures, guidance and templates for GDPR readiness	The Council has appropriate governance arrangements in place to continue to share information compliantly with partners when GDPR becomes enforceable
Business Continuity & Disaster Recovery	The Council requires a high level of assurance around business continuity and disaster recovery arrangements for critical systems	95% of Council systems have been risk assessed	The Council understands where its business critical systems are	Joint working with Business Continuity & Emergency Planning to make sure that appropriate arrangements are in place for resilience	The Council understands its assets and can continue to work and recover in the event of an incident
Training, Culture & Awareness	Changes to Data Protection law will mean that the Council's Online Data Protection training course requires updating	IG Group have begun reviewing and updating content, in line with available guidance from regulator	Online training will be redesigned and finalised by the end of the last quarter of 2017	All Staff will be required to undertake appropriate training to refresh their knowledge in the first quarter of 2018	Our Staff have the right knowledge to play their role in the appropriate use and governance of the Council's information and data
	Refreshed and joined up Information Governance related training in place for Elected Members	Joint working between IG Group, Committee Services & Organisational Development to design and plan appropriate sessions	Information Governance training sessions for Elected Members in place for September 2017	Use feedback from sessions to manage and improve further training or guidance required by Elected Members	Our Elected Members have the right knowledge to play their role in the appropriate use and governance of the Council's information and data
Information	Council's response to Scottish Child Abuse	IG Group agreed Retention Schedule be	Corporate Records Retention Schedule	IG Group will continue monitor and update the	The Council is retaining its information in

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Preservation	Inquiry prompted review of retention periods for Council Policy	updated with revised retention period for all Council Policy	revised and updated	Corporate Records Retention Schedule in response to changing legislative or business requirements	accordance with changing legal and business requirements
Strategic Performance Management & Transformation	The Council has a fragmented understanding of its customers because of lack of data integration between key systems	Master Data Management Hub and Integration layer business requirements developed. Logical Data model developed	The Council is ready to procure a Master Data Management Hub and Integration layer	Procurement and implementation of MDM hub and Integration layer	The Council has the capability required to integrate its data about people and place
Realising Information Re-use Value	The Council wants to open up its non-personal data wherever possible to the benefit of its people, economy and place	Open Data Standards have been developed as part of the National Open Data Programme the Council is a part of. The Council has established an open data working group	The Council is working collaboratively to build the foundations required for a sustainable open data programme	Open Data Platform to be implemented and regular open data publishing schedule to be agreed	The Council is opening up its data to benefit the people, place and economy of Aberdeen

3. Information Governance Performance Information July 2016- June 2017

3.1 Data Protection Act 1998

3.1.1 Data Protection Requests

Fig.1: Annual number of requests received

Type of Request	12 months to June 2017	12 months to June 2016
Subject Access Requests	144	100
Third Party Requests	604	350

Fig. 2: Number of requests received over the last 12 months

Fig. 3: Requests received by Directorate

Directorate	Subject Access Request	Third Party Request	TOTAL
Aberdeen City Health & Social Care Partnership	36	86	122
Communities, Housing & Infrastructure	9	267	276
Corporate Governance	19	125	144
Education & Children's Services	71	80	151
Office of the Chief Executive	0	0	0
Joint H&SCP E&CS	9	46	55

Data Protection Act 1998 in brief

The Data Protection Act 1998 (DPA) regulates the Council's role, rights and responsibilities in the use, management and protection of our customers' (staff and the public) personal data.

Subject Access Requests

Anyone who we hold personal data about can ask us for a copy of it.

Third Party Requests

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

Commentary on number of requests received

The number of reported requests has increased by 66% compared with the same period 12 months ago, partly attributable to the Information Governance Group ensuring that all TPR are centrally reported, as follows:

CH&I have been logging CCTV requests since September 2016.

Third Party Requests to the Archive Service have been included in the statistics from July 2016.

Fig. 4: Corporate compliance with timescales for requests

Type of Request	12 months to June 2017	12 months to June 2016
Subject Access Requests	68%	72%
Third Party Requests	97%	94%
Total compliance	91%	89%

Timescales for responding

The Council must provide the personal information requested for SARs within 40 calendar days.

Commentary on compliance

Combined compliance with timescales for SARs and TPRs has been consistent over the past 12 months; however the compliance rates for SARs have improved considerably over the course of this year.

The majority of Data Protection requests are TPRs which tend to be for limited information which can be delivered quickly. SARs for social care records often involve sifting and redacting large and complex case files.

Fig. 5: Corporate compliance with timescales over the last 12 months

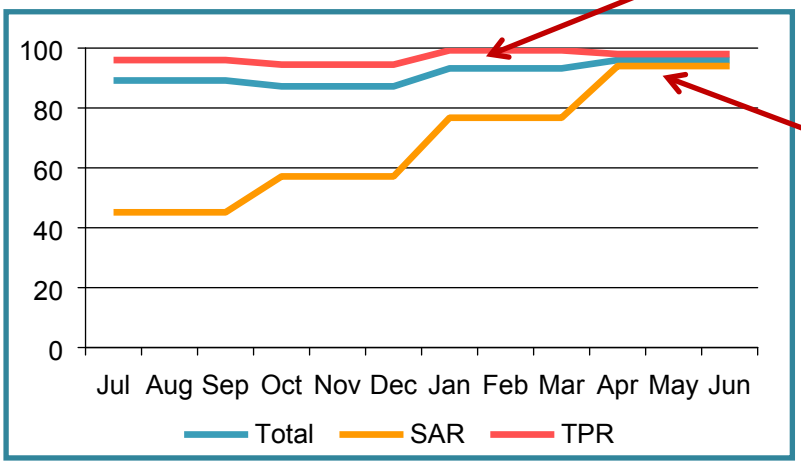


Fig. 6: Compliance with timescales by Council Directorate

Directorate	On time	Late
Aberdeen City Health & Social Care Partnership	91	19
Communities, Housing & Infrastructure	271	1
Corporate Governance	138	0
Education & Children's Services	106	24
Office of the Chief Executive	0	0
Joint H&SCP E&CS	48	4

Late requests

Late requests are those requests closed in the reporting period which exceeded the 40 day calendar day response time.

Commentary on compliance by Directorate

The reasons for late responses are the nature and extent of the workload in the team providing a response, and a large volume of information and complexity of files to be checked and sometimes redacted.

3.1.2 Data Protection Breaches and Complaints

Fig. 7: Annual breaches and data handling complaints

Breaches	12 months to June 2017	12 months to June 2016
Breaches	35	30
Self-Reports to the ICO	0	6
Data Handling Complaints	0	3

Fig. 8: Breaches by type over the last 12 months

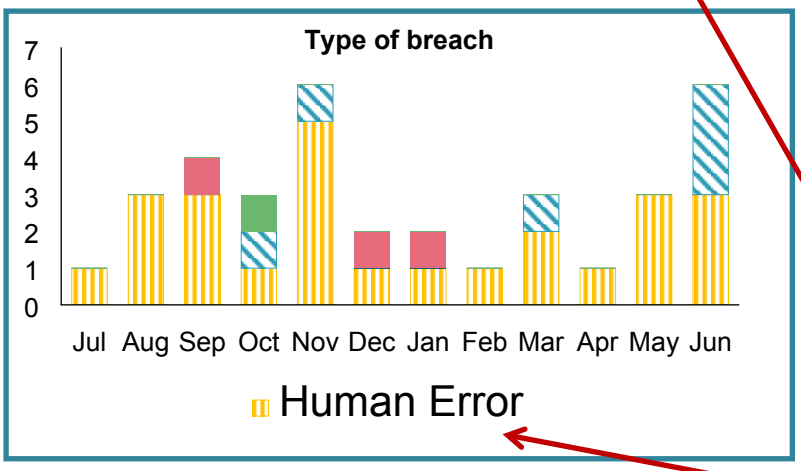
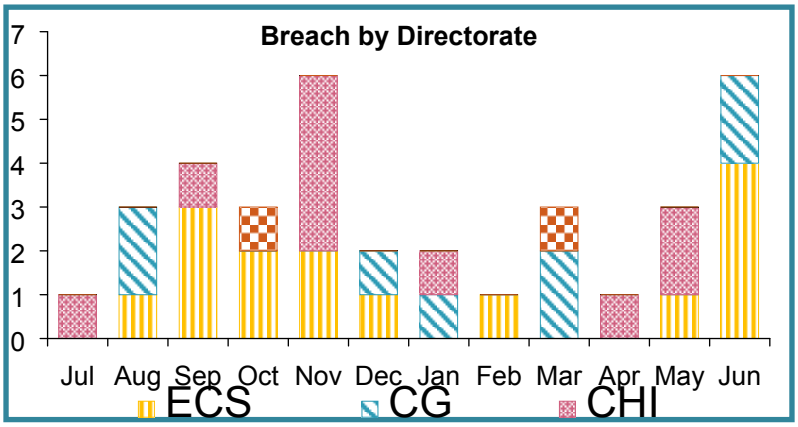


Fig. 9: Breaches by Directorate in the period



Data Protection Breaches

All potential breaches should be reported in line with the Council's procedures. The action taken will depend on the nature of the breach.

Self-Reportable Breaches

Where the nature of a breach poses significant actual or potential detriment to individuals the Council should self-report to the ICO.

Data Handling Complaints

Anyone who is unhappy with the way that the Council has handled their personal data can make a complaint to us. If they are unhappy with our response to their complaint they may escalate their complaint to the ICO.

Commentary on number and type of breaches

This year has seen an increase on breaches compared to the previous period. Human error continues to be the most common cause.

Analysis of the underlying causes has been the focus of the Information Governance Group and this has informed the shape and content of the 'Information Matters' awareness campaign which is running in September 2017.

Online Data Protection training for all staff will be revised and updated for GDPR in the last quarter of 2017 and all staff will be required to refresh and update their knowledge in the first quarter of 2018 in readiness for the 25 May 2018 when GDPR becomes enforceable.

3.2 Freedom of Information (Scotland) Act 2002 & Environmental Information (Scotland) Regulations 2004

3.2.1 FOISA and EIR Information Requests

Fig 10: Annual number of requests received in the period

Number of requests received	12 months to June 2017	12 months to June 2016
Number of FOISA Requests	1335	1102
Number of EIR Requests	466	485

Fig 11: Request numbers in the last 12 months

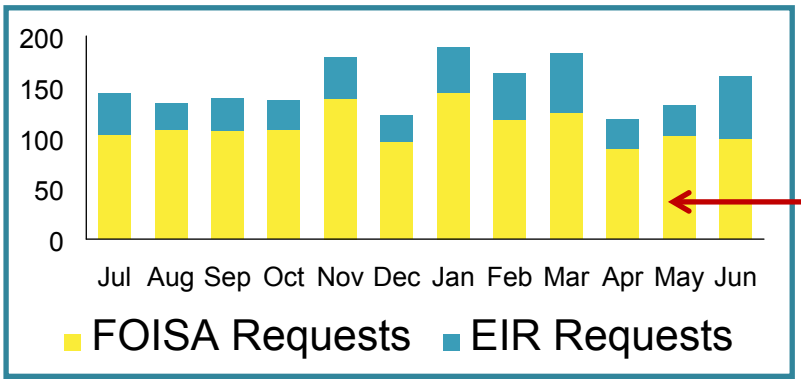
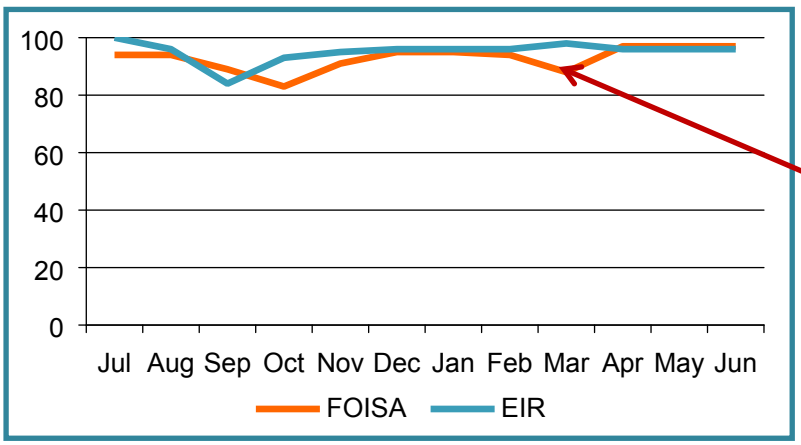


Fig 12: Compliance with timescales in the period

Requests responded to within timescale	12 months to June 2017	12 months to June 2016
FOISA Requests	93%	93%
EIR Requests	95%	91%

Fig 13: Compliance with timescales in the last 12 months (%)



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.

Commentary on request numbers

Request numbers continue to increase year on year. The dips in request s received over holiday periods are consistent with previous years. There was a significant drop in the total number of requests in April and May (possibly due to Scottish and General Elections). There was also an increase in EIR requests in June due, in part, to the fire at Grenfell Tower, London. Other areas of requests include, in Education, topics such as bullying, violent incidents and restraint techniques and, in Land & Property, topics such as statutory notices and inspection reports.

Commentary on compliance

Annual compliance with timescales for FOI requests has averaged 93% over the past 12 months. There was a drop in compliance in March 2017 for FOI requests relating to Procurement and Social Care.

A more efficient approval process is now in place for requests which require checking from the Media Team. Additional support has been provided to the Information Compliance Team to allow officers to focus on tackling possible delays and to provide advice to services in a timely manner.

3.2.2 FOISA and EIR Request Internal Reviews

Fig. 14: Internal Reviews received by type in the period

Type of review received	12 months to June 2017	12 months to June 2016
No response received	6	13
Unhappy with response	20	20

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.

Fig.15: Internal Review Panel outcomes in the period

Type of review outcome	12 months to June 2017	12 months to June 2016
Response upheld	14	15
Response overturned or amended	9	10

Internal Review Panels

Where a requester is unhappy with our response, an internal review panel will decide whether to uphold the Council's response or to overturn or amend it.

3.2.3 FOISA and EIR Request Appeals

Fig. 16: FOISA and EIR Appeals received and closed in the period

No. of Appeals	12 months to June 2017	12 months to June 2016
Received	8	5
Closed	7	5

The 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.

Fig. 17: FOISA and EIR Appeal outcomes in the period

Appeal Outcomes	12 months to June 2017	12 months to June 2016
Council response upheld	3	2
Lateness	1	2
Council response overturned	3	1

Commentary on Appeals

There is one ongoing appeal concerning the Hazlehead Crematorium internal investigation report. Information Governance Group will consider any issues arising from this appeal.

1 appeal concerned lateness in relation to Financial Assessment information and it was found that ACC was required to respond.

3 responses were overturned, relating to fees charged to access planning information; confidentiality; commercial sensitivity. The fees charged for accessing planning information have now been reviewed and revised. Information about Investments and Pensions has been released as required.

3.3 Information Security

3.3.1 Cyber Incidents

Fig. 18: Overview of cyber incidents in the period

Incident Type	12 months to June 2017	12 months to June 2016
Internal Cyber Incident Attempts	1	Consolidated figures for comparison are not available
Internal Cyber Incidents	6	
External Cyber Incident Attempts	18089194	
External Cyber Incidents	5	

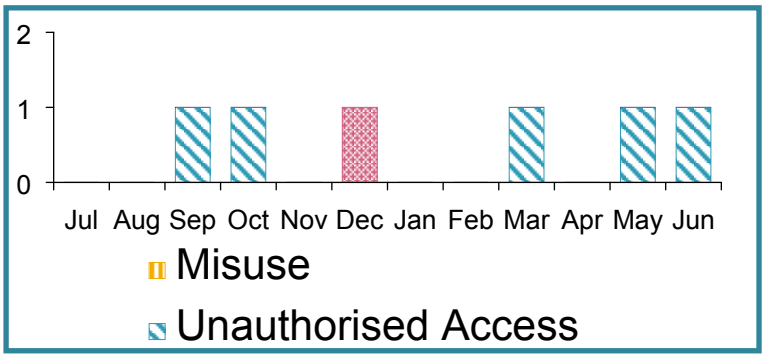
Information Security in brief

The Council is responsible for the integrity, confidentiality and availability of its information. The Council protects it from internal and external threats by using all available controls, and ensuring that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised.

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.

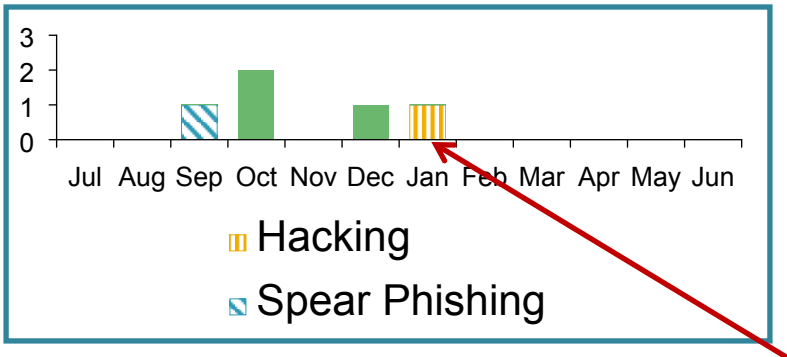
Fig. 19: Internal Cyber Incidents in the period



Commentary on Internal Cyber Incidents

These incidents included password relaying at a school, a compromised Google account, a copyright infringement, web page defacement, and a security issue caused by non-ACC equipment compromising the network. These incidents were mitigated, and did not have a significant impact on business. Appropriate remedial action was taken in each case.

Fig. 20: External Cyber Incidents



External Cyber Incidents

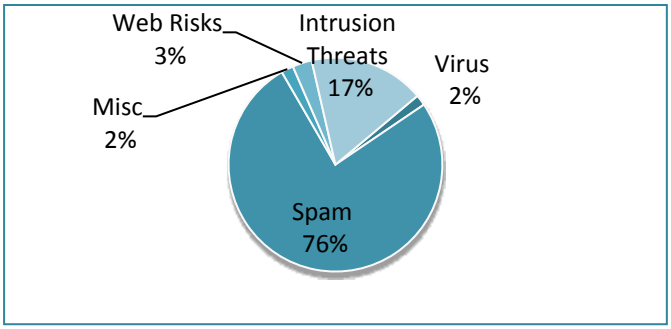
These are risks or threats to the Council's information software, infrastructure or computer network that originate from outside the premises or from the public (e.g. hackers)

Commentary on External Cyber Incidents

In January the corporate website home page was hacked and defaced. This was managed as a major incident which was subject to separate reports to this Committee.

Other incidents in this period were mitigated, and did not have a significant impact on business. Appropriate remedial action was taken in each case.

Fig. 21: Breakdown of External Cyber Incident attempts in the period



3.3.2 Physical Incidents

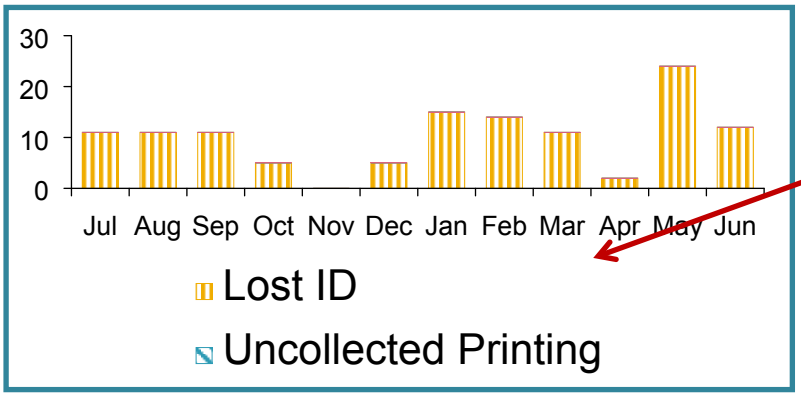
Fig. 21: Physical Incidents in the period

Incident Type	12 months to June 2017	12 months to June 2016
Internal Physical Incidents	121	No figure for comparison
External Physical Incidents	74	76

Internal Physical Incidents

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

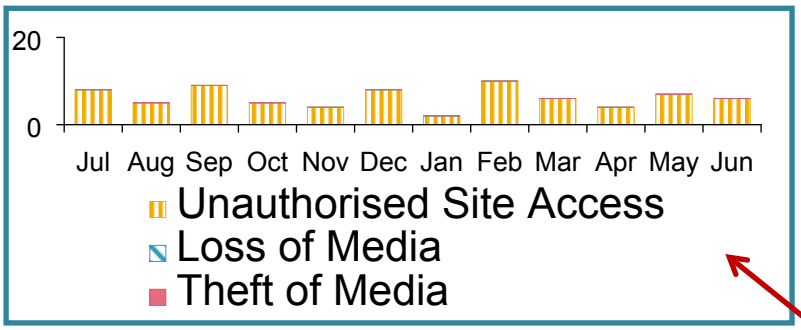
Fig. 22: Internal Physical Incidents by type in the period



Commentary on Internal Physical Incidents

The roll-out of the new printing contract across the estate reduced the security risk associated with uncollected printing by implementing the default secure printing setting.

Fig 23: External Physical Incidents by type in the period



External Physical Incidents

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

Commentary on External Physical Incidents

The number of reported incidences of unauthorised site access is similar to and down very slightly on the same period 12 months ago.

Further information about these instances is collected via Health & Safety reporting.