Local Government Association

Research

Response and Recovery Survey 2023

Report of findings

December 2023

To view more research from the Local Government Association Research and Information team please visit: https://www.local.gov.uk/our-support/research

Contents

Executive Summary

This report outlines the findings of a survey of local councils on their preparedness to deal with a cyber incident. The purpose of the survey was to provide the Local Government Association (LGA) with a baseline on which to build its Cyber, Digital and Technology programme and ensure that local authorities have the support they most need to respond to the increasing cyber threat.

Background

The LGA conducted an online survey of councils between September and November 2023 via an individual link emailed to Heads of Information Technology (IT) in all councils in England. In total, 59 responses were received, representing a response rate of 19 per cent due to the number of responses from councils with shared services.

Key messages

Cyber incident response planning

- Almost all (95 per cent) of the councils who took in the survey have a plan, or plans, to help them respond and recover in the event of a cyber incident.
- The most commonly reported types of plans were (respondents could select more than one answer):
    - IT prioritised recovery plan/business continuity plan (BCP) (64 per cent);
    - Organisation wide business continuity plan (BCP) (57 per cent);
    - Organisation wide cyber incident response plan (43 per cent), and;
    - Departmental/Service wide IT disaster recovery plan (DRP) (43 per cent).
- Most plans included the following (respondents could select more than one answer):
    - Defined rules and responsibilities (79 per cent);
    - Named incident response team (71 per cent), and;
    - Post incident review (70 per cent).
- The respondents whose plans included a communications strategy reported that these most commonly included the following components (respondents could select more than one answer):
    - Channels to communicate with staff in the event of a total loss of IT (43 per cent);
    - Internal communications principles (41 per cent), and;
    - Media statements and materials (27 per cent).
- Most respondents (86 per cent) would be able to access their plans if there was a total loss of IT.

- Almost all respondents (98 per cent), reported that contact details for key personnel who will handle the response to an incident would be accessible if there was a total loss of IT.
- Just 14 per cent of respondents stated that they used bespoke/third-party software to support their business continuity management.

Development of cyber incident plans

- Plans had been developed strategically based on identified/potential risks in 46 per cent of respondent councils while 43 per cent reported that theirs had developed organically over time.
- The factors most commonly cited as informing the development of cyber incident plans were (respondents could select more than one answer):
    - Cyber incident exercises and testing (75 per cent);
    - A cyber incident at another council/organisation (66 per cent), and;
    - Changes in legislation (55 per cent).
- The senior management team members most commonly reported to be involved in the development of cyber incident plans were:
    - Chair of Information Governance Board/Senior Information Risk Owner (SIRO) (86 per cent - 25 per cent to a great extent, 29 per cent to a moderate extent and 33 to a small extent);
    - Director of Corporate Services (incl. Finance) (71 per cent – 7 per cent to a great extent, 22 per cent to a moderate extent and 44 to a small extent), and;
    - Chief Executives, with over half (59 per cent) involved (5 per cent to a great extent, 13 per cent to a moderate extent and 41 to a small extent).

Incident response

- The duties of the cyber incident response team had been explained to those who would be undertaking them in most respondent councils (88 per cent), and training had been provided in just under half (46 per cent).
- There was no testing of the duties of the cyber incident response team by those undertaking them in 39 per cent of respondent councils. A quarter (25 per cent) tested them every year, 9 per cent did it every six months and 4 per cent tested every two years.
- A fifth (21 per cent) of respondent councils provided cyber incident response training to staff outside of the cyber incident response team.
- Most respondents (82 per cent) had multiple copies of their backup systems, with one offline/cold or immutable copy. The same proportion (82 per cent) stated that their backups were created frequently, and 80 per cent reported that they were held on at least two devices, with one offsite or offline.

- Just over half of respondent councils (54 per cent) had arrangements in place to bring in external support, such as an NCSC assured cyber incident response company, if required.
- Half of respondents (52 per cent) carried out tests and exercises of their cyber incident plans, with just under half of these (45 per cent), carrying out tests and exercises every year. The scenarios most commonly covered were phishing (86 per cent) ransomware (79 per cent), and suspicious account activity (52 per cent).
- The IT Team was involved in cyber incident exercises and tests in most respondent councils (93 per cent), followed by the cyber incident response and emergency planning teams (69 per cent each).
- Tests and exercises covered containment, eradication and recovery in 83 per cent of respondent councils, while post-incident activity, including impact management and detection, and analysis were both covered by 69 per cent.

Cyber security arrangements

- Just 7 per cent of respondent councils had experienced hostile cyber incidents over the last three years, which led to unexpected costs or resourcing requirements.
- Most respondent councils (90 per cent) log, and bring together, security information from across their networks for analysis while 63 per cent had a Security Incident & Event Management solution (SIEM)
- Half (49 per cent) of respondents with a SIEM solution paid a fixed licensing cost for using it while 27 per cent paid a variable cost, based on the amount of data uploaded and five per cent paid both a fixed and variable cost.
- A quarter (24 per cent) of respondent councils reported that they had a Security Operations Centre (SOC). This was delivered through an external organisation in almost two-thirds (64 per cent) of councils and while in a fifth (21 per cent) it was delivered internally through the IT team.
- Just two (14 per cent) of the respondent councils with a SOC shared it with another council. One reported that there was a total of ten councils sharing in their SOC while the other reported their total as six.
- Most (79 per cent) of the respondents who had a SOC thought that cyber security at their council improved since its introduction, mostly in relation to monitoring.
- Among respondents with a SOC almost two-thirds (64 per cent) had 24-hour cover each day to deal with security incidents identified by its SOC. Costs and the scope of their contracts were cited as reasons for not having this in place by those without 24-hour cover each day.
- Please note that as only a very small number of respondents had a SIEM solution and even fewer had a SOC, these findings should be treated with caution and cannot be seen as representative of all councils.

Introduction

About the survey

This report outlines the results of a survey undertaken by the LGA to build a better understanding of how prepared the local government sector is to respond to a cyber incident. The findings will be used to shape the LGA's Cyber, Digital and Technology programme and ensure that local authorities have the support they most need to respond to the increasing cyber threat.

Methodology

An online survey was conducted via an individual link circulated to Heads of IT in all councils in England, and was in the field between 12 September and 8 November 2023. Two reminders were sent during this period. Information about the survey was also circulated via networks and in relevant bulletins to ensure that IT leads were aware of it.

A total of 59 responses were received from all types of council, including those who share their services, representing 19 per cent of councils. This level of response means that these results should not be taken to be more widely representative of all councils. Rather, they are a snapshot of this particular group of respondents.

The information collected by the survey has been aggregated, and no individuals or authorities are identified in this report. Throughout the report, percentages in figures and tables may add to more than 100 per cent due to rounding. Sample size figures are shown in tables to allow readers to see the basis on which the figures have been calculated.

Where the response base is less than 50, care should be taken when interpreting percentages, as small differences can seem magnified. Therefore, where this is the case in this report, absolute numbers are reported alongside the percentage values.

Responses

Table 1 shows the number responses received broken down by council type.

Table 1: Responses by type of authority

Type of authority	Number of responses	Per cent
District	28	17%
County	5	24%
London borough	5	15%
Metropolitan district	7	20%
Unitary	12	19%
Councils with shared services	6	n/a

Base: All respondents (59)

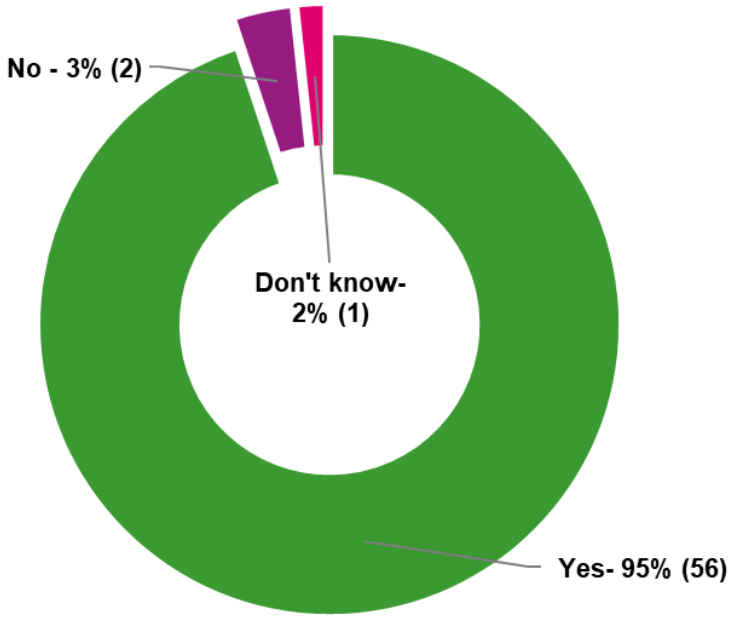
Survey findings

This section outlines the full set of survey results.

Cyber incident response planning

Almost all (95 per cent) of the councils who took in the survey have a plan, or plans, to help them respond and recover in the event of a cyber incident. Just three per cent did not have a plan, while a further two per cent of respondents didn't know whether they had any plans. These findings are shown in Figure 1.

Figure 1: Does your council have a plan, or plans, to help it respond and recover in the event of a cyber incident?

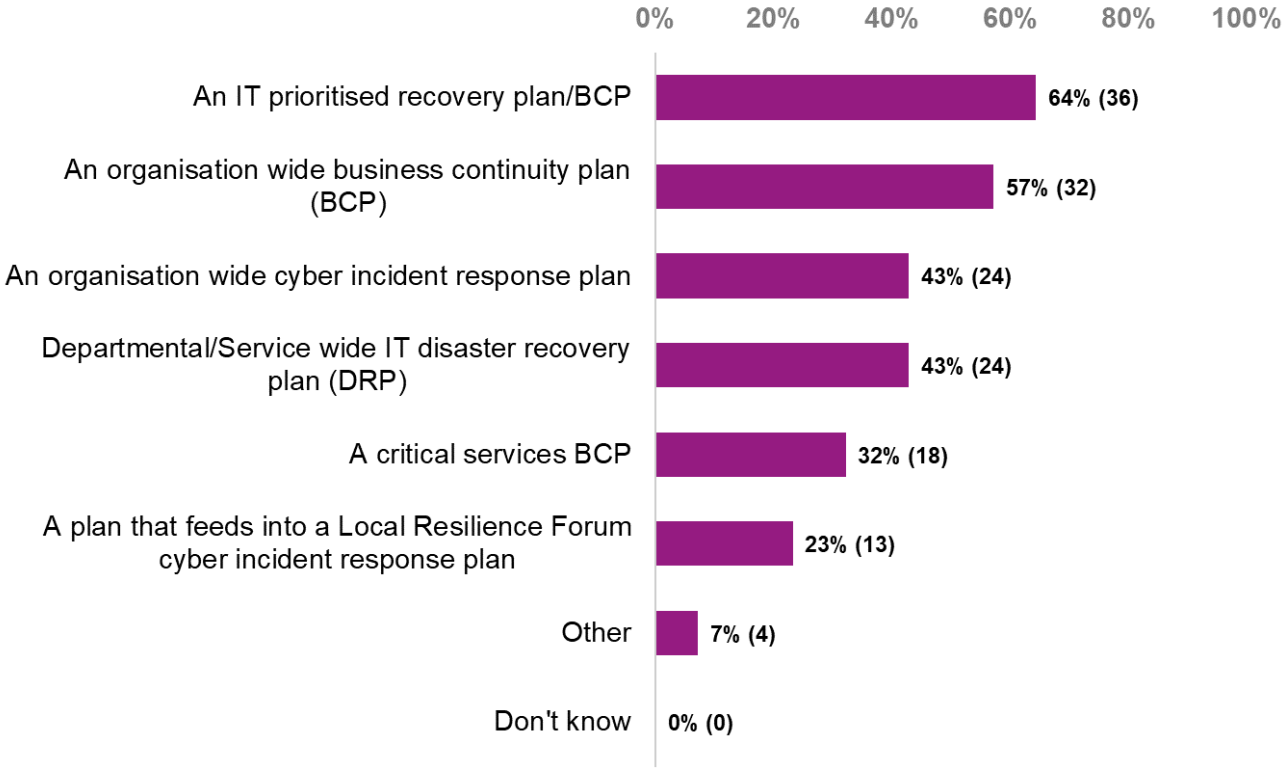


Base: all respondents (59)

Respondents with plans were asked to indicate what type of plans they had, using a list of descriptions provided. The most commonly selected type of plan, chosen by 64 per cent of respondents, was an IT prioritised recovery plan/ business continuity plan (BCP), this was followed by an organisation wide business continuity plan (BCP), selected by 57 per cent, while both an organisation wide cyber incident response plan and Departmental/Service wide IT disaster recovery plan (DRP) were chosen by 43 per cent of respondents. Figure 2 illustrates these findings and a full breakdown of the responses to this question can be seen in Table 2.

The respondents who selected the 'other' were asked to specify what this meant, the answers given included that their plans had not yet been finalised and that in addition to types of plans listed, they also had departmental BCPs, a major incident response plan, a cyber security incident response plan, and a DR Plan. A list of all the answers provided is shown in Table A1 in Annex A.

Figure 2: Which of the following most closely describes your council's cyber incident response plan/plans?



Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 2: Which of the following most closely describes your council's cyber incident response plan/plans?

Answer	Number of responses	Per cent
An IT prioritised recovery plan/BCP	36	64%
An organisation wide business continuity plan (BCP)	32	57%
An organisation wide cyber incident response plan	24	43%
Departmental/Service wide IT disaster recovery plan (DRP)	24	43%
A critical services BCP	18	32%
A plan that feeds into a Local Resilience Forum cyber incident response plan	13	23%
Other	4	7%
Don't know	0	0%

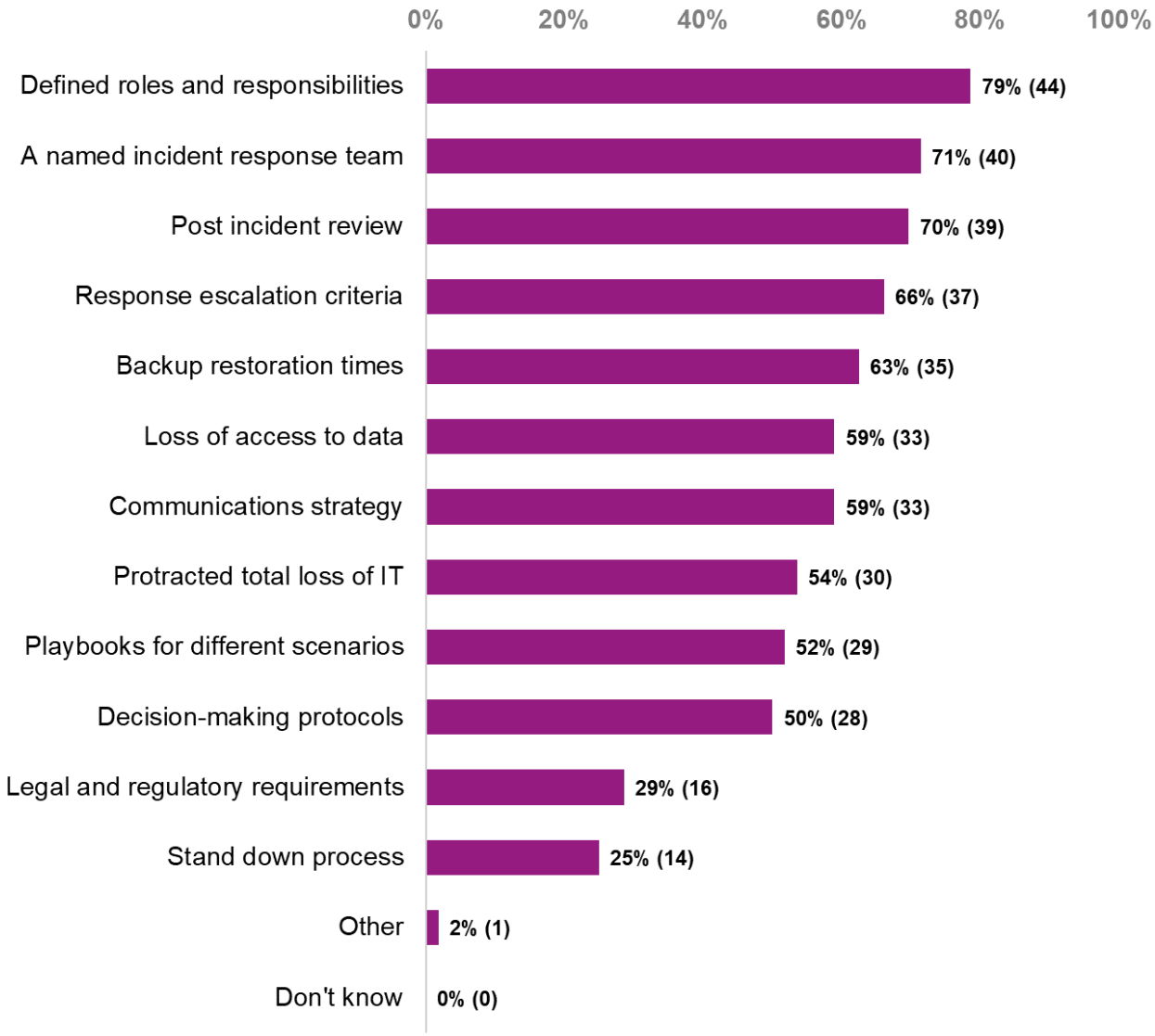
Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Respondents with a plan were then asked to specify what was included in their plans by selecting components from a list provided. Four in five respondents (79 per cent) chose defined rules and responsibilities, this was followed by a named incident

response team (71 per cent) and post incident review (70 per cent), as the most commonly selected components.

Half of respondents (50 per cent) selected decision making protocols, while legal and regulatory requirements and stand down 29% were chosen by 29 per cent and 25 per cent, respectively, making these the least commonly selected components. The respondent who selected the other category reported that their plan included links to the LRF locally and coordination with partners. Figure 3 shows these findings and a full breakdown of the responses is listed in Table 3.

Figure 3: Which of the following are included in your council's cyber incident plan/plans?



Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 3: Which of the following are included in your council's cyber incident plan/plans?

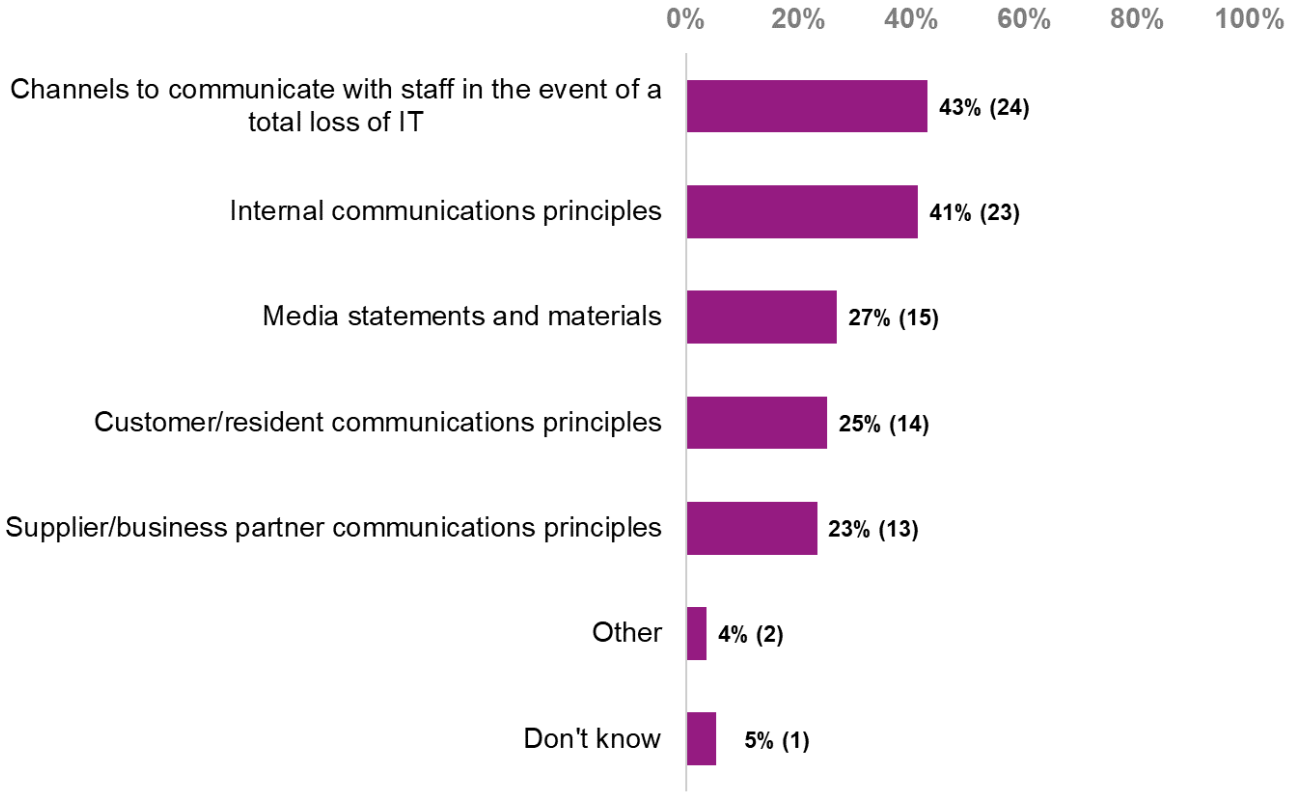
Answer	Number of responses	Per cent
Defined roles and responsibilities	44	79%
A named incident response team	40	71%
Post incident review	39	70%
Response escalation criteria	37	66%
Backup restoration times	35	63%
Loss of access to data	33	59%
Communications strategy	33	59%
Protracted total loss of IT	30	54%
Playbooks for different scenarios	29	52%
Decision-making protocols	28	50%
Legal and regulatory requirements	16	29%
Stand down process	14	25%
Other	1	2%
Don't know	0	0%

Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

The respondents who indicated that their plans included a communications strategy were asked to provide further information about what was included, by once again selecting components from a list provided. The most commonly chosen components were channels to communicate with staff in the event of a total loss of IT, selected by 43 per cent, internal communications principles (41 per cent) and media statements and materials (27 per cent).

These findings are illustrated in Figure 4 and are listed in Table 4. As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils. The answers given by the two respondents who selected 'other' are shown in Table A2 in Annex A.

Figure 4: Which of the following are included in your council's cyber incident communications strategy?



Base: Respondents whose cyber incident plans include a communications strategy (33)
Note: Respondents could select more than one answer

Table 4: Which of the following are included in your council's cyber incident communications strategy?

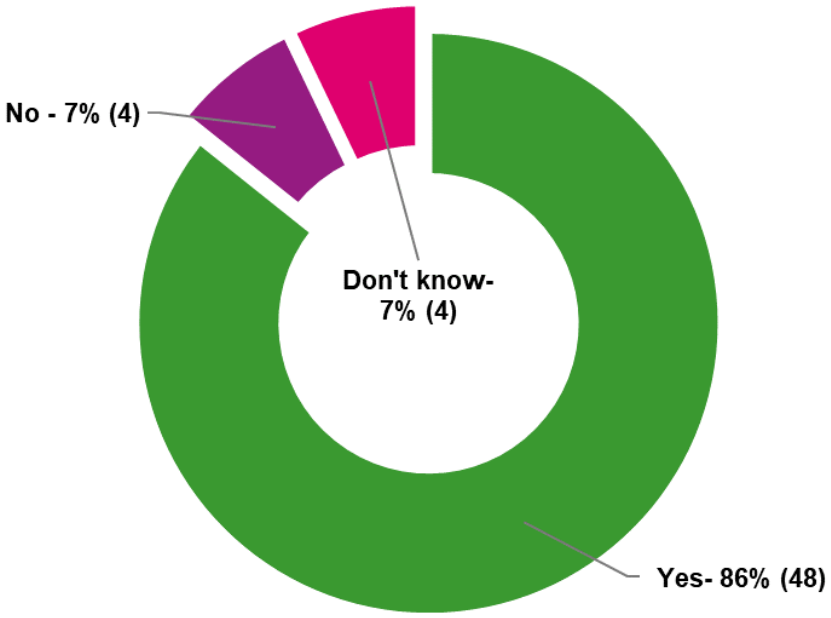
Answer	Number of responses	Per cent
Channels to communicate with staff in the event of a total loss of IT	24	43%
Internal communications principles	23	41%
Media statements and materials	15	27%
Customer/resident communications principles	14	25%
Supplier/business partner communications principles	13	23%
Other	2	4%
Don't know	3	5%

Base: Respondents whose cyber incident plans include a communications strategy (33)
Note: Respondents could select more than one answer

A small number of respondents provided further details about their council's cyber incident communications strategy. Two reported on the current status of their strategies while the others provided details of how theirs worked in practice. All of the answers provided can be seen in Table A3 in Annex A.

Most respondents (86 per cent) would be able to access their plans if there was a total loss of IT. Just seven per cent would be unable to do so, while a further seven per cent didn't know if they would be able to access their plans. These findings can be seen in Figure 5.

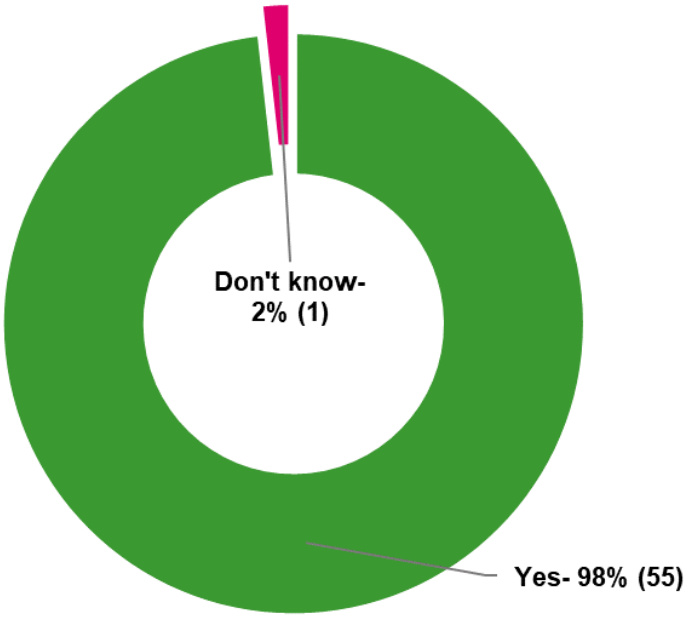
Figure 5: Would your council's cyber incident plan/plans be accessible if there was a total loss of IT?



Base: Respondents with cyber incident plans (56)

Almost all respondents (98 per cent) reported that contact details for key personnel who will handle the response to an incident would be accessible if there was a total loss of IT. No respondents said they would not be accessible but one (2 per cent) did not know. These findings are illustrated in Figure 6.

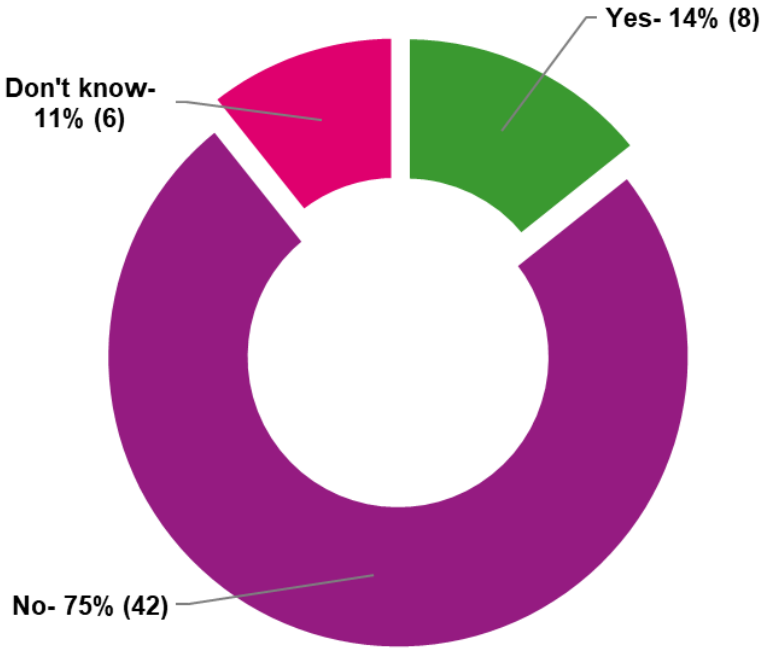
Figure 6: Would contact details for key personnel who will handle the response to an incident be accessible if there was a total loss of IT?



Base: Respondents with cyber incident plans (56)

As shown in Figure 7, just 14 per cent of respondent councils said that they used bespoke/third-party software to support their business continuity management, three quarters (75 per cent) did not and 11 per cent didn't know whether they used it.

Figure 7: Does your council use bespoke/third-party software to support business continuity management?



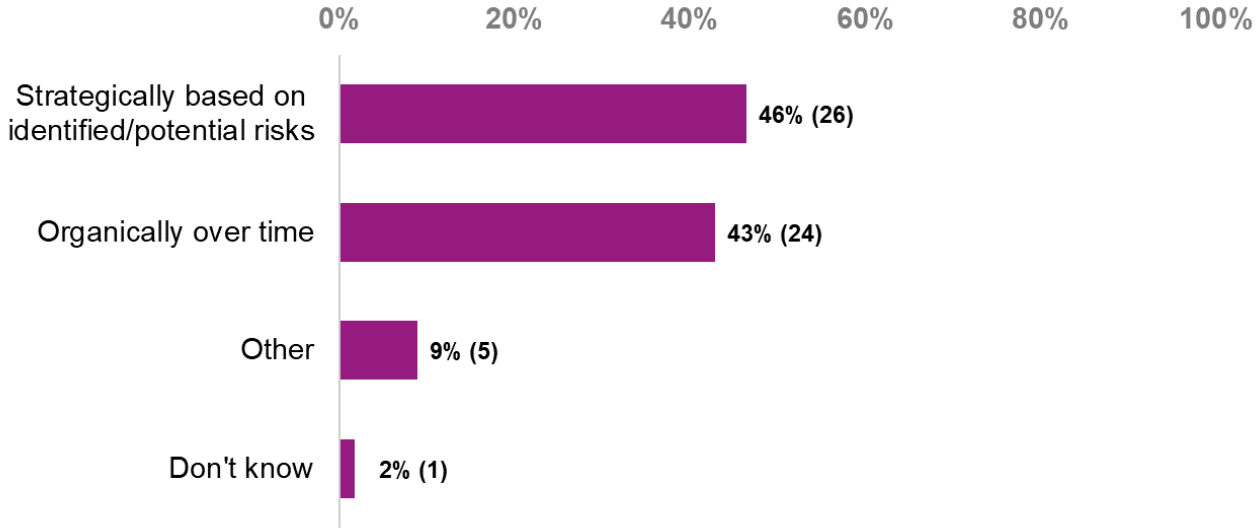
Base: Respondents with cyber incident plans (56)

A small number of respondents provided further details about their plans. Their comments included information about where their plans sat within wider emergency planning, testing, and details around how they intended to develop their plans. All the answers provided are shown in Table A4 in Annex A.

Development of cyber incident plans

There was a fairly even split between respondents in terms of how their plans had been developed, with 46 per cent stating it had been done strategically based on identified/potential risks and 43 per cent reporting theirs had developed organically over time. A further nine per cent answered that theirs had developed in other ways, these included in partnership with IT providers, with support from the LGA and following a particular methodology. These findings are illustrated in Figure 8 and a full list of the other ways plans were developed is shown in Table A5 in Annex A.

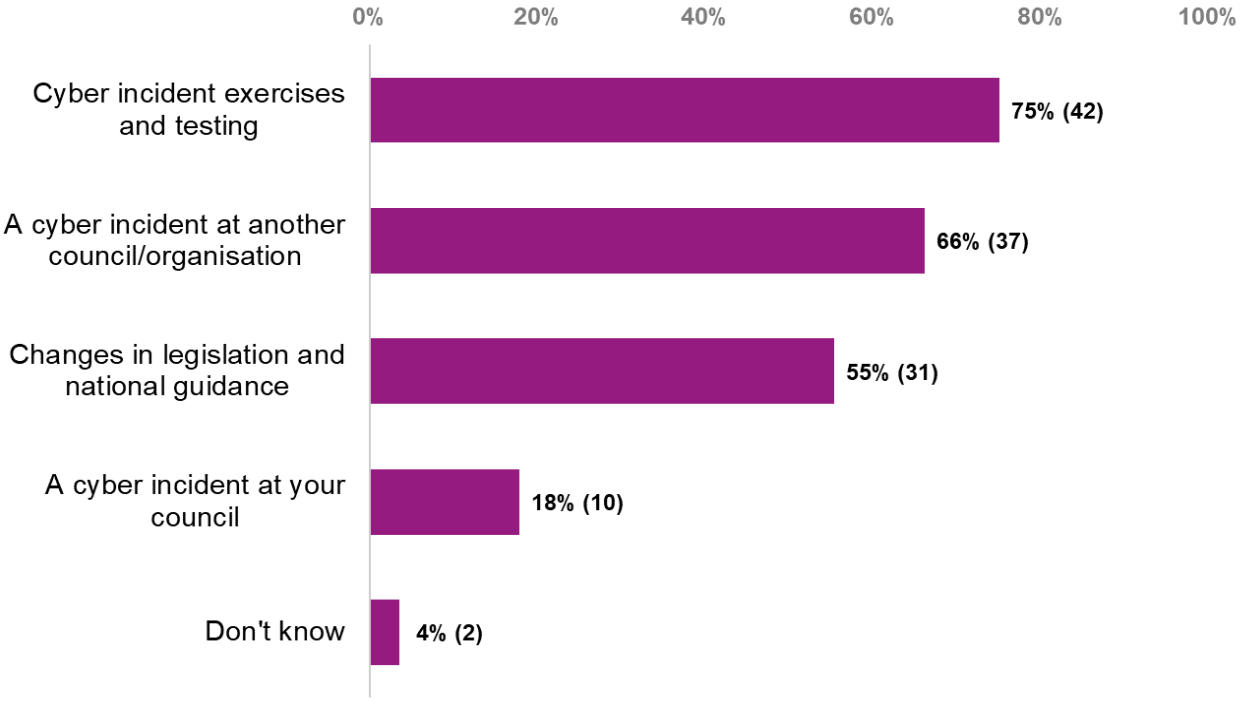
Figure 8: How was your council's cyber incident plan/plans developed?



Base: Respondents with cyber incident plans (56)

Respondents were asked to indicate what had informed the development of their cyber incident plans using a list provided. Three quarters (75 per cent) chose cyber incident exercises and testing, two-thirds (66 per cent) selected a cyber incident at another council/organisation and 55 per cent selected changes in legislation and national guidance (25 per cent). Just eight per cent chose a cyber incident at their council while four per cent didn't know, as shown in Figure 9 and Table 5.

Figure 9: Did any of the following inform the development of council's cyber incident plan/plans?



Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 5: Did any of the following inform the development of council's cyber incident plan/plans?

Answer	Number of responses	Per cent
Cyber incident exercises and testing	42	75%
A cyber incident at another council/organisation	37	66%
Changes in legislation and national guidance	31	55%
A cyber incident at your council	10	18%
Don't know	2	4%

Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

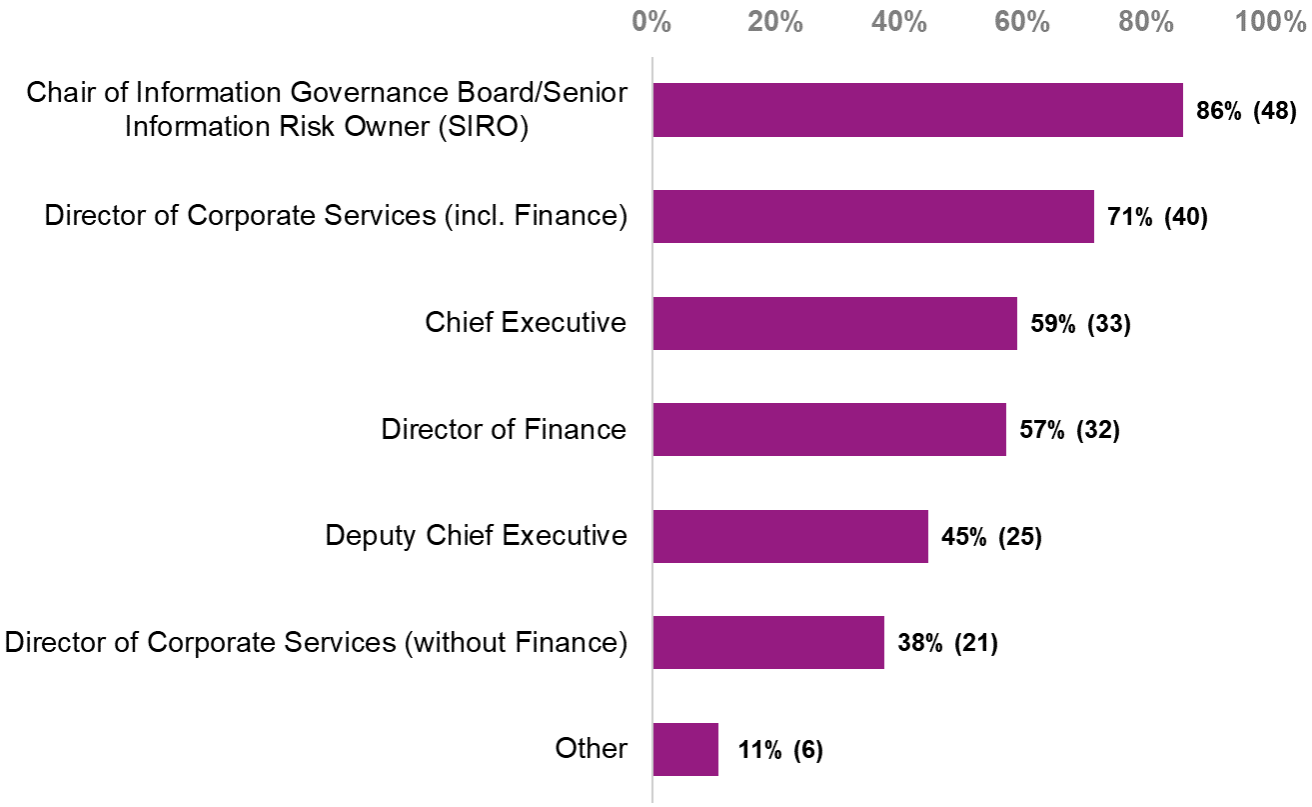
When asked about their senior management team's involvement in the development of their cyber incident plans, most respondents (86 per cent) reported that the Chair of Information Governance Board/Senior Information Risk Owner (SIRO) had been involved (25 per cent to a great extent, 29 per cent to a moderate extent and 33 to a small extent). The next most commonly involved senior managers were Directors of Corporate Services (incl. Finance) (71 per cent – 7 per cent to a great extent, 22 per cent to a moderate extent and 44 to a small extent) and Chief Executives with over half (59 per cent) involved (5 per cent to a great extent, 13 per cent to a moderate extent and 41 to a small extent).

The respondents who reported that other members of their senior management team were involved were asked to specify their job titles, the answers provided included Assistant Chief Executive (where the deputy chief executive had also been involved), Chief Operating Officer and Assistant Director Policy Strategy & Resources. A full list of the job titles provided can be found in Table A6 in Annex A.

Figure 10 illustrates the involvement of senior managers in the development of cyber incident plans, with a breakdown also shown in Table 6, while Table 7 provides a full breakdown of the extent of their involvement.

Further details provided about the development of respondents' cyber incident plans included comments about how they had been developed, future development of the plans and details around their senior management team's involvement. All answers provided can be seen in Table A7 in Annex A.

Figure 10: Involvement of senior managers in the development of cyber incident plans in respondent councils



Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 6: Involvement of senior managers in the development of cyber incident plans in respondent councils

Answer	Number of responses	Per cent
Chair of Information Governance Board/Senior Information Risk Owner (SIRO)	48	86%
Director of Corporate Services (incl. Finance)	40	71%
Chief Executive	33	59%
Director of Finance	32	57%
Deputy Chief Executive	25	45%
Director of Corporate Services (without Finance)	21	38%
Other	6	11%

Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 7: To what extent was the council's senior management team involved in the development of its cyber incident plan/plans?

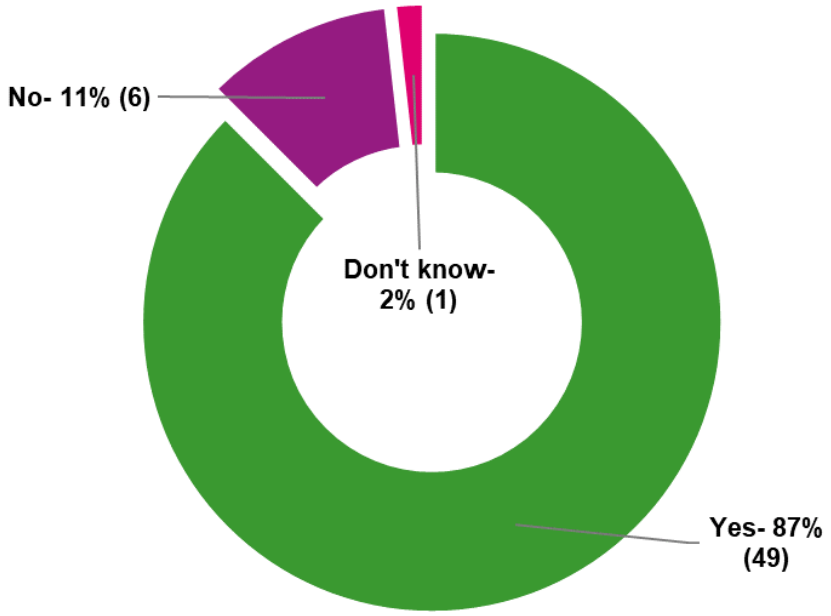
	To a great extent	To a moderate extent	To a small extent	Not at all	Don't know	Total
Chair of Information Governance Board /Senior Information Risk Owner (SIRO)	25% (14)	29% (16)	33% (18)	9% (5)	4% (2)	55
Director of Corporate Services (incl. Finance)	7% (4)	22% (12)	44% (24)	19% (10)	7% (4)	54
Chief Executive	5% (3)	13% (7)	41% (23)	34% (19)	7% (4)	56
Director of Finance	4% (2)	16% (8)	44% (22)	28% (14)	8% (4)	50
Deputy Chief Executive	8% (4)	12% (6)	30% (15)	36% (18)	14% (7)	50
Director of Corporate Services (without Finance)	2% (1)	16% (7)	29% (13)	31% (14)	22% (10)	45
Other	60% (3)	20% (1)	20% (2)	0% (0)	0% (0)	6

Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Incident response

The duties of the cyber incident response team had been explained to those who would be undertaking them in most respondent councils (88 per cent). However, this was not the case for one in ten (11 per cent) respondent councils while a further two per cent did not know, as shown in Figure 11.

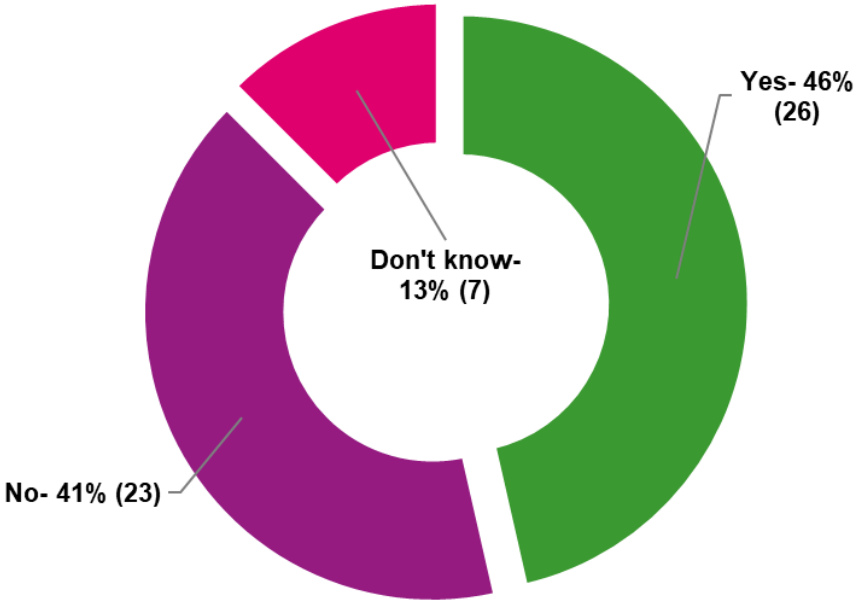
Figure 11: Are the duties of the cyber incident response team explained to those undertaking them?



Base: Respondents with cyber incident plans (56)

Training in the duties of the cyber incident response team had been provided in just under half of respondent councils (46 per cent). It had not been provided in 41 per cent and 13 per cent of respondents did not know whether or not this training had been provided. These findings can be seen in Figure 12.

Figure 12: Has training been provided in the duties of the cyber incident response team?



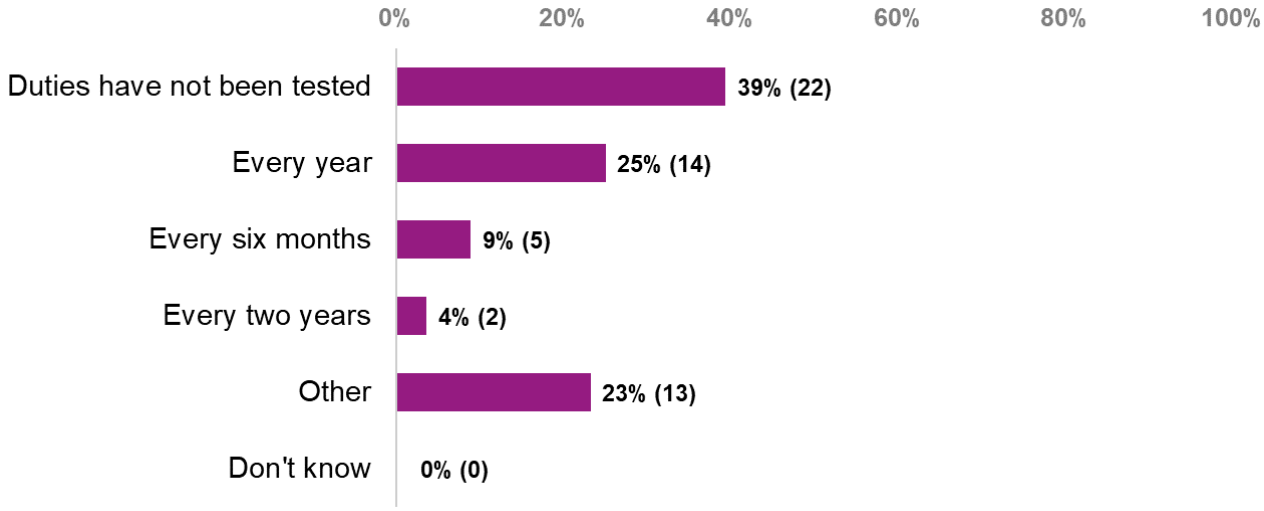
Base: Respondents with cyber incident plans (56)

Testing of the duties of the cyber incident response team by those undertaking them had not taken place in 39 per cent of respondent councils. A quarter (25 per cent) did this testing every year, nine per cent did it every six months and four per cent tested every two years. These findings are illustrated in Figure 13 and are listed in Table 8.

Those who answered 'other' were asked to specify the frequency at which they tested, their answers included monthly, bi-monthly, every three months, and on an ad hoc basis. All the answers provided are listed in Table A8 in Annex A.

The small number of respondents who gave further details about their cyber incident response teams all provided clarification on their answers in relation to testing, where this had not taken place. Their answers can be seen in Table A9 in Annex A.

Figure 13: How often, if at all, are the duties of the cyber incident response team tested by those undertaking them?



Base: Respondents with cyber incident plans (56)

Table 8: How often, if at all, are the duties of the cyber incident response team tested by those undertaking them?

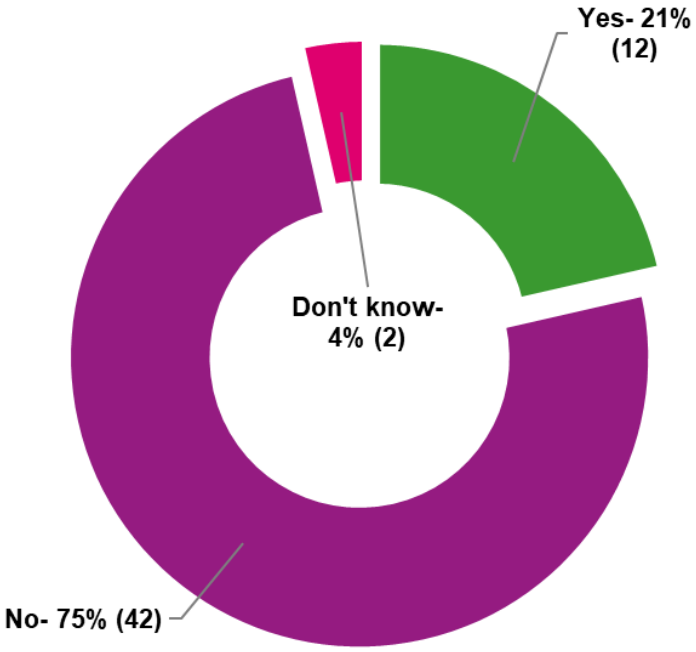
Answer	Number of responses	Per cent
Duties have not been tested	22	39%
Every year	14	25%
Every six months	5	9%
Every two years	2	4%
Other	13	23%
Don't know	0	0%

Base: Respondents with cyber incident plans (56)

Cyber incident response training had not been provided to staff outside of the cyber incident response team in 84 per cent of respondent councils. Just 21 per cent had

provided this training while four per cent of respondents did not know if training had been provided to staff outside of the cyber incident response team. Figure 14 shows these findings.

Figure 14: Has cyber incident response training been provided to staff outside of the cyber incident response team?



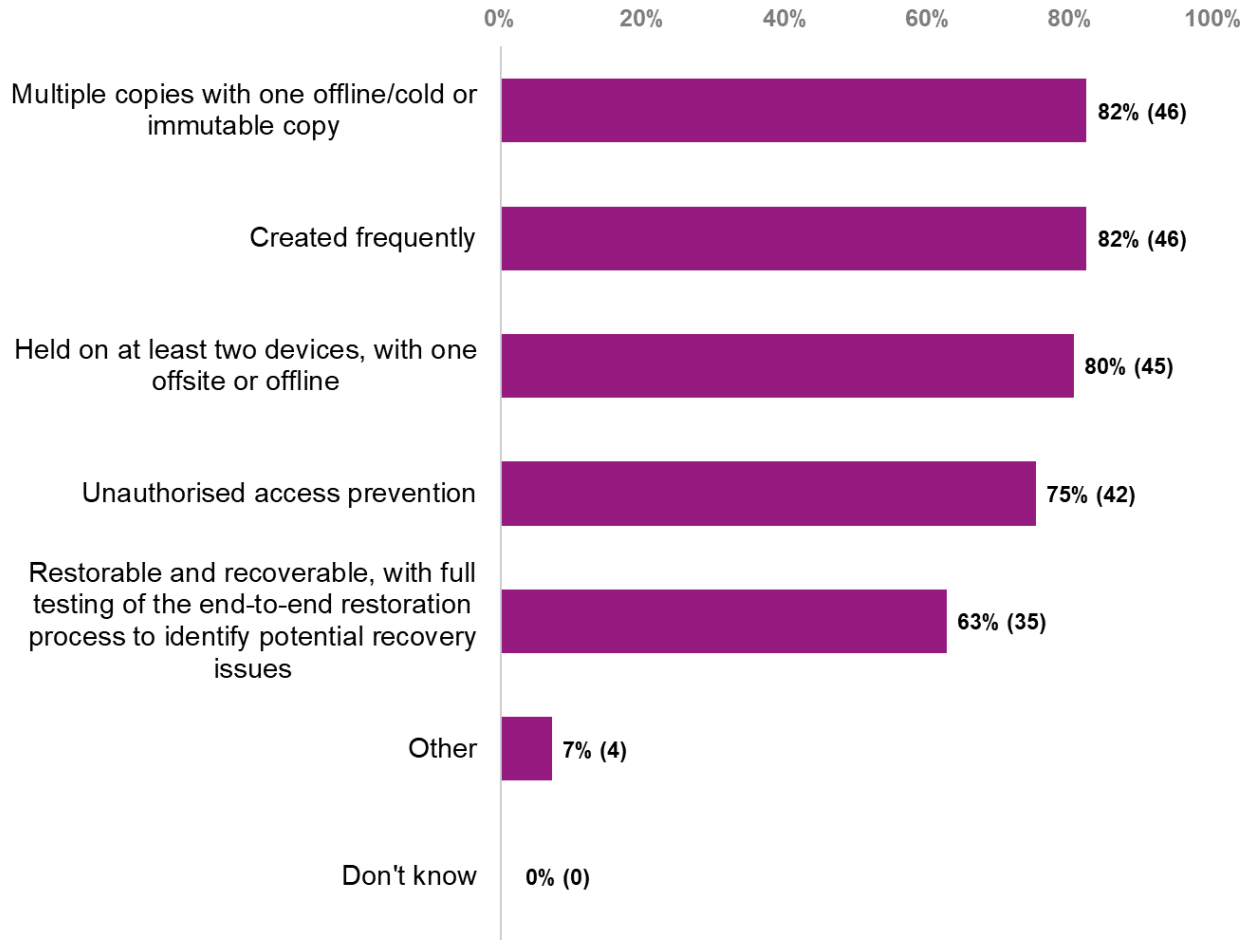
Base: Respondents with cyber incident plans (56)

Respondents who had provided cyber incident response training to staff outside of the cyber incident response team were asked to specify who had received it. Staff identified included heads of service, business continuity leads and wider IT team members. All of the answers provided can be found in Table A10 in Annex A.

When asked to indicate which components of a list provided applied to their backup systems respondent councils most commonly reported that they had multiple copies with one offline/cold or immutable copy, that backups were created frequently (82 per cent each), and that they were held on at least two devices, with one offsite or offline (80 per cent). Figure 15 shows these findings, which are also displayed in Table 9.

The councils who indicated that they had something else in place were asked to specify this, the answers provided included that backups were wholly cloud hosted, partly immutable, and different types of restoration and testing were in place. A list of all the other answers provided is shown in Table A11 in Annex A.

Figure 15: Which of the following, if any, apply to your council's backup system?



Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Table 9: Which of the following, if any, apply to your council's backup system?

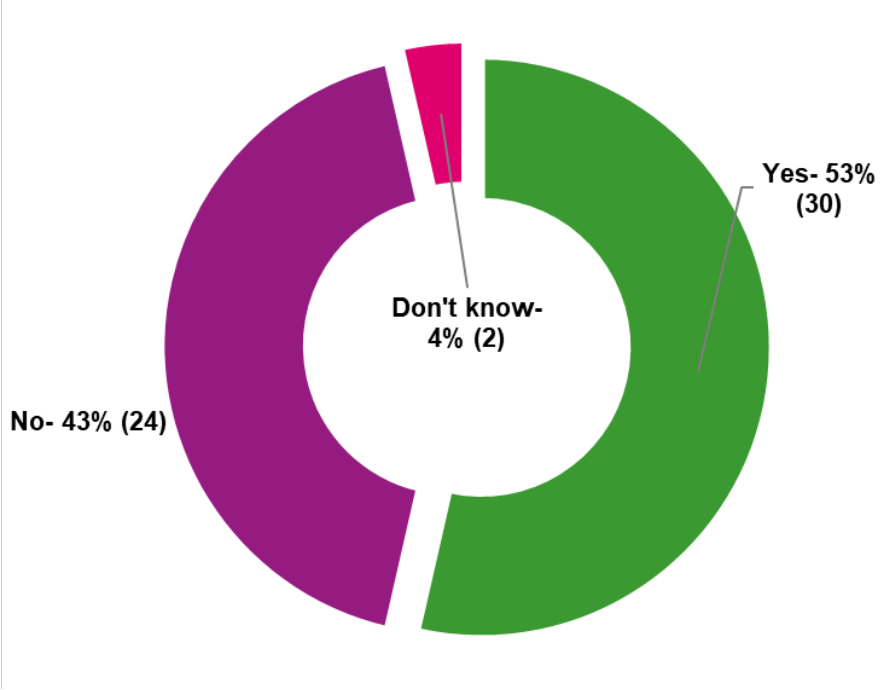
Answer	Number of responses	Per cent
Multiple copies with one offline/cold or immutable copy	46	82%
Created frequently	46	82%
Held on at least two devices, with one offsite or offline	45	80%
Unauthorised access prevention	42	75%
Restorable and recoverable, with full testing of the end-to-end restoration process to identify potential recovery issues	35	63%
Other	4	7%
Don't know	0	0%

Base: Respondents with cyber incident plans (56) Note: Respondents could select more than one answer

Just over half of respondents (54 per cent) reported that they had arrangements in place to bring in external support, such as an NCSC assured Cyber Incident Response (CIR) company, if required. There were no such arrangements in place at 43 per cent of respondent councils while four per cent did not know if they had these arrangements. This findings can be seen in Figure 16.

When asked to provide further details about their council's preparations, respondents mostly commented about the current status of their progress in this area as well as providing additional details about their local arrangements. All of the answers given are shown in Table A12 in Annex A.

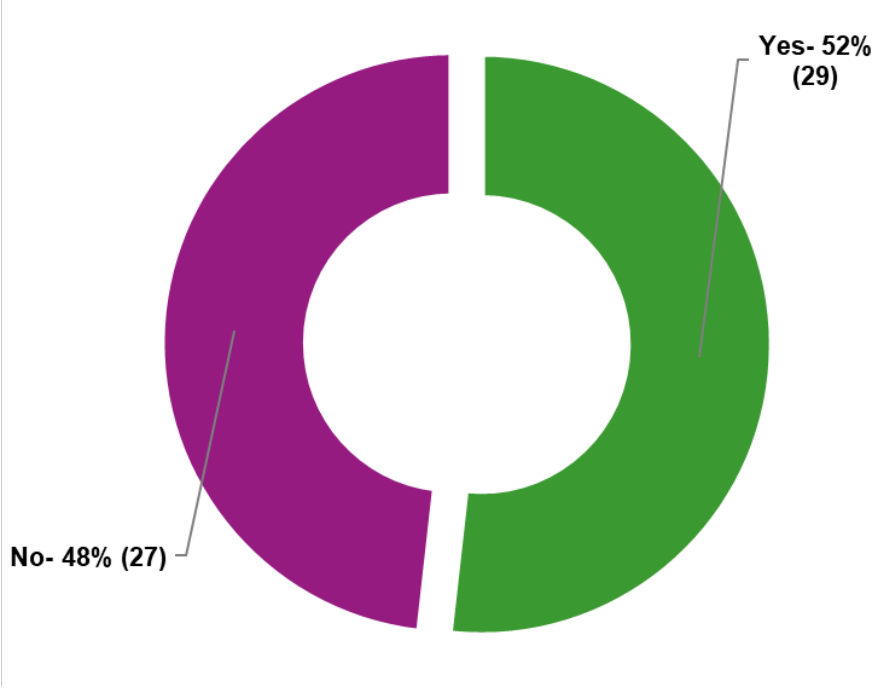
Figure 16: Does your council have arrangements in place to bring in external support, such as an NCSC assured Cyber Incident Response company, if required?



Base: Respondents with cyber incident plans (56)

Respondents were fairly evenly split in terms of carrying out tests and exercises of their cyber incident plan/plans with half (52 per cent) reporting they did this with the other half (48 per cent) stating they did not test their plans, as shown in Figure 17.

Figure 17: Does your council carry out tests and exercises of its cyber incident plan/plans?



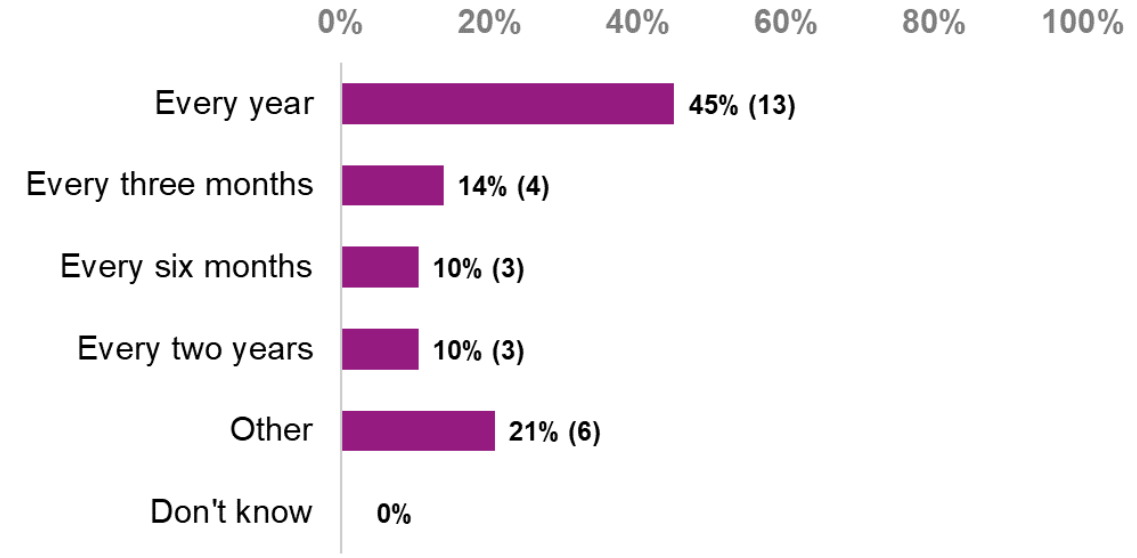
Base: Respondents with cyber incident plans (56)

Among the respondent councils who carry out cyber incident testing and exercising the most common frequencies were every year (45 per cent) and every three months (14 per cent) followed by every six months and every two years (10 per cent each). Figure 18 shows these findings and they are listed in Table 10.

Answers specified by those who reported testing at other frequencies included every month, every other month and randomly, to reflect the real-world. All of the other answers provided can be seen in Table A13 in Annex A.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 18: How frequently is cyber incident testing and exercising undertaken?



Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Table 10: How frequently is cyber incident testing and exercising undertaken?

Answer	Number of responses	Per cent
Every year	13	45%
Every three months	4	14%
Every six months	3	10%
Every two years	3	10%
Other	6	21%
Don't know	0	0%

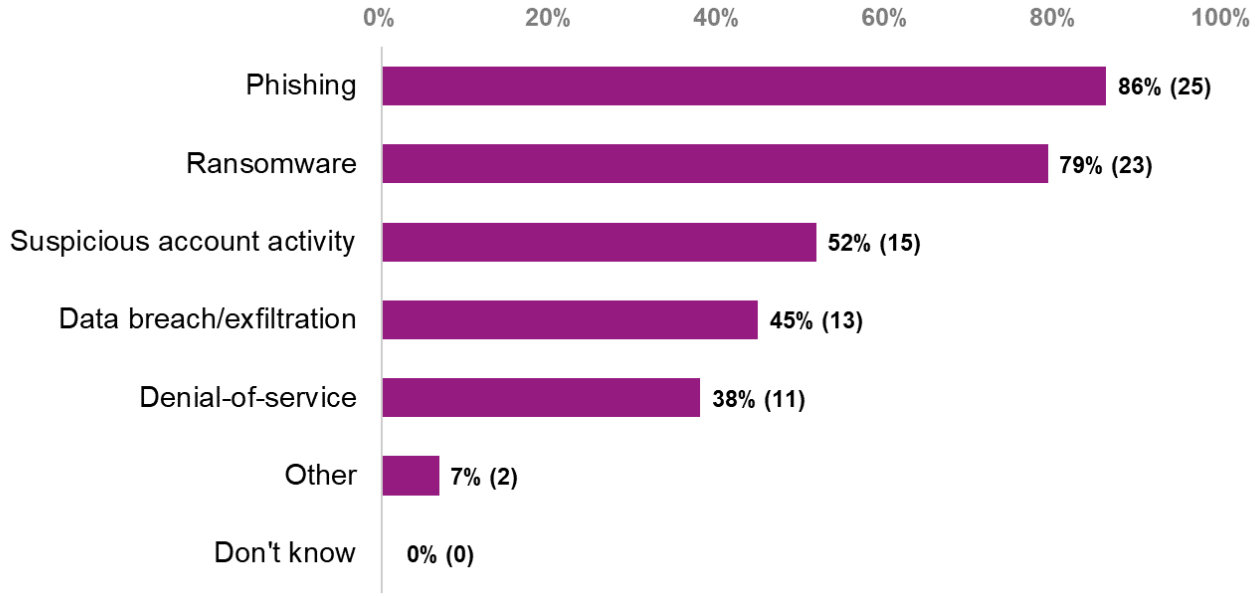
Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

The scenarios most commonly covered in survey respondent council's cyber incident exercises and tests were phishing (86 per cent), ransomware (79 per cent) and suspicious account activity (52 per cent). A breakdown of these findings is shown in Figure 19 and they are listed in Table 11.

The scenarios covered in the two respondent councils who tested in other areas included BYOD, third party software compromise and chain security. The answers they provided are shown in full in Table A14 in Annex A.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 19: Which of the following scenarios have been covered in your council's cyber incident exercises and tests?



Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Table 11: Which of the following scenarios have been covered in your council's cyber incident exercises and tests?

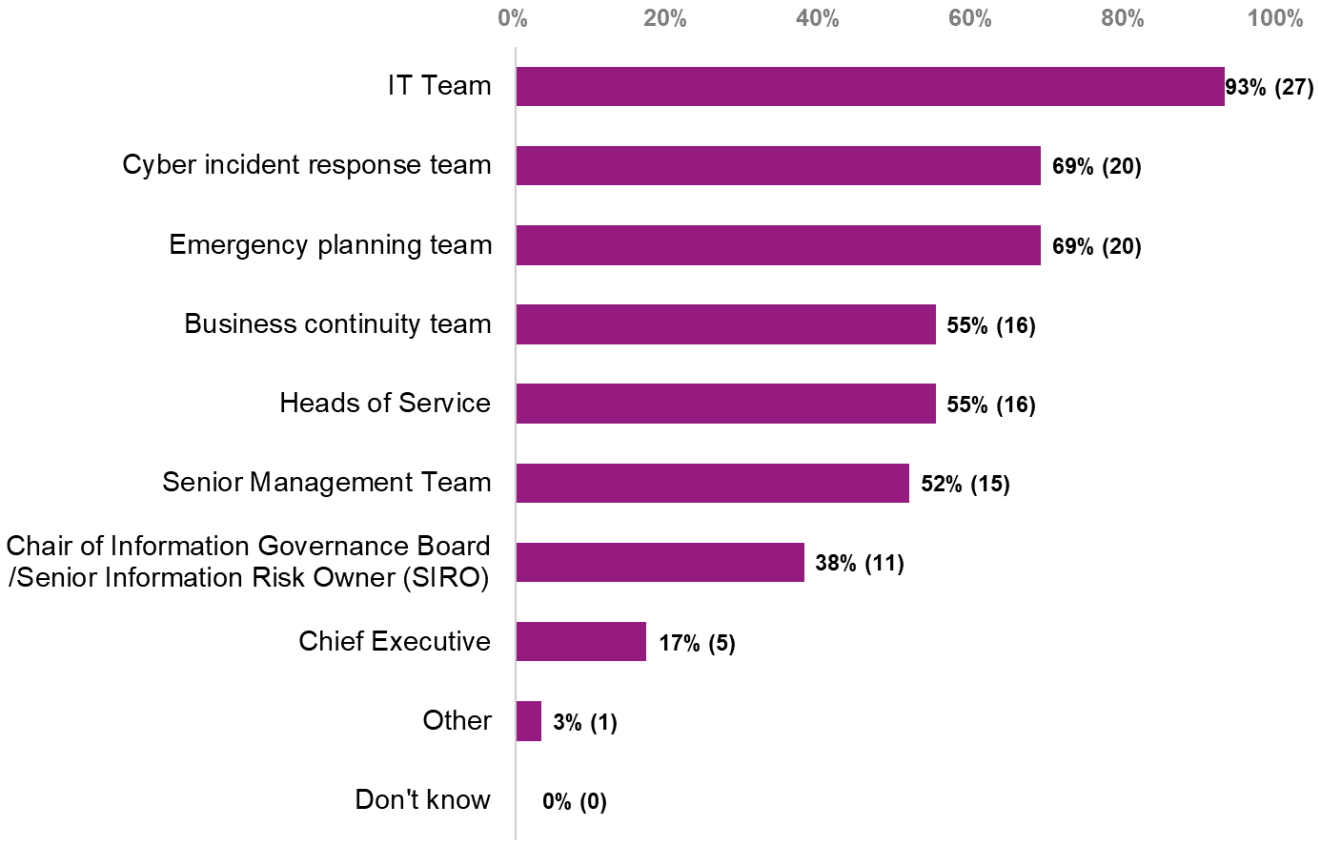
Answer	Number of responses	Per cent
Phishing	25	86%
Ransomware	23	79%
Suspicious account activity	15	52%
Data breach/exfiltration	13	45%
Denial-of-service	11	38%
Other	2	7%
Don't know	0	0%

Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Among respondent councils it was most common for the IT Team (93 per cent) to be involved in their cyber incident exercises and tests, followed by the cyber incident response and emergency planning teams (69 per cent each). Figure 20 provides a full breakdown of these findings, which are also listed in Table 12.

The respondent who answered 'other' specified this as the Director of IT and the Transformation Director. As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 20: Who is involved in your council's cyber incident exercises and tests?



Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Table 12: Who is involved in your council's cyber incident exercises and tests?

Answer	Number of responses	Per cent
IT Team	27	93%
Cyber incident response team	20	69%
Emergency planning team	20	69%
Business continuity team	16	55%
Heads of Service	16	55%
Senior Management Team	15	52%
Chair of Information Governance Board /Senior Information Risk Owner (SIRO)	11	38%
Chief Executive	5	17%
Other	1	3%

Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Most respondents (83 per cent) reported that they covered containment, eradication and recovery in their exercises and tests while post-incident activity, including impact

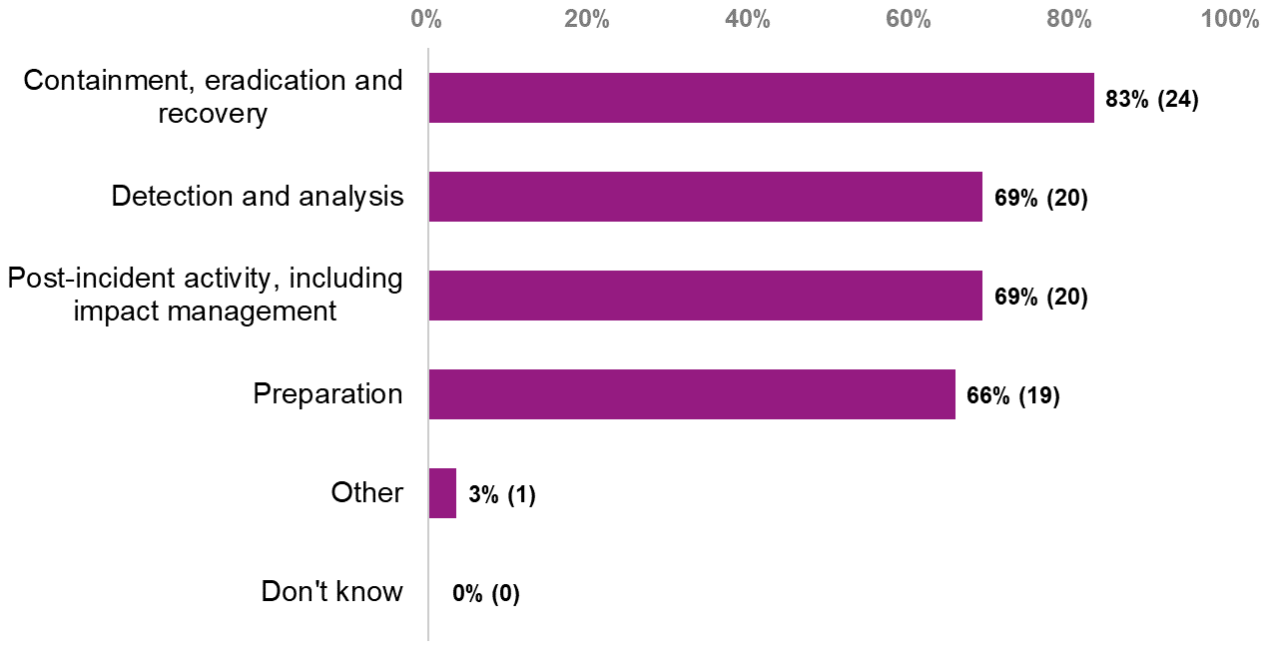
management and detection, and analysis were both covered by 69 per cent. These findings are shown in Figure 21 and listed in Table 13.

The respondent who answered 'other' provided this detail:

> "Our Incident Response Plan was designed based on the Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned (PICERL) methodology."

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 21: Which parts of the cyber incident response cycle are covered by your council's exercises and tests?



Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Table 13: Which parts of the cyber incident response cycle are covered by your council's exercises and tests?

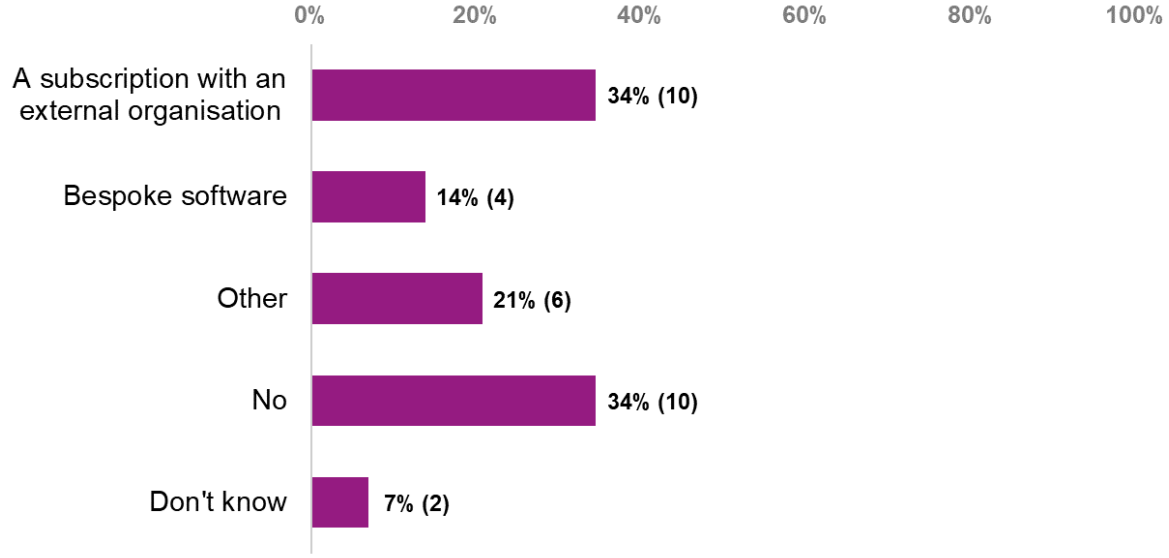
Answer	Number of responses	Per cent
Containment, eradication and recovery	24	83%
Detection and analysis	20	69%
Post-incident activity, including impact management	20	69%
Preparation	19	66%
Other	1	3%
Don't know	0	0%

Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

A third of respondent councils (34 per cent) who carry out cyber incident testing and exercising had a subscription with an external organisation to conduct business continuity and/or cyber security exercises while 14 per cent used bespoke software. A fifth (21 per cent) reported using other means, these included NCSC exercises in a box, WARP events and commercially available cyber simulations. These findings are shown in Figure 22 and Table 14. The details provided by respondents who answered 'other' can be found in Table A15 in Annex A.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 22: Does your council use any of the following to conduct business continuity and/or cyber security exercises?



Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Table 14: Does your council use any of the following to conduct business continuity and/or cyber security exercises?

Answer	Number of responses	Per cent
A subscription with an external organisation	10	34%
Bespoke software	4	14%
Other	6	21%
No	10	34%
Don't know	2	7%

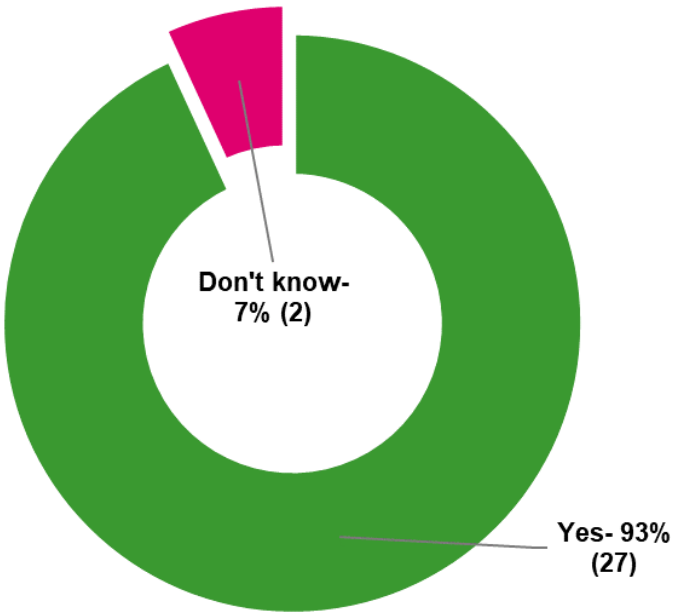
Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Most (93 per cent) of the respondent who carried out exercises and tests used the lessons learnt from these exercises and tests to update their council's cyber incident

plans. No respondents reported that they did not do this, but two (7 per cent) did not know whether this happened. Figure 23 illustrates these findings. As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

A small number of respondents provided further details about their council's cyber exercises and tests when given the opportunity. Their comments all related to the status of their plans including details of their plans for future exercises and tests. All of the answers provided can be seen in Table A16 in Annex A.

Figure 23: Are the lessons learnt from exercises and tests used to update your council's cyber incident plan/plans?



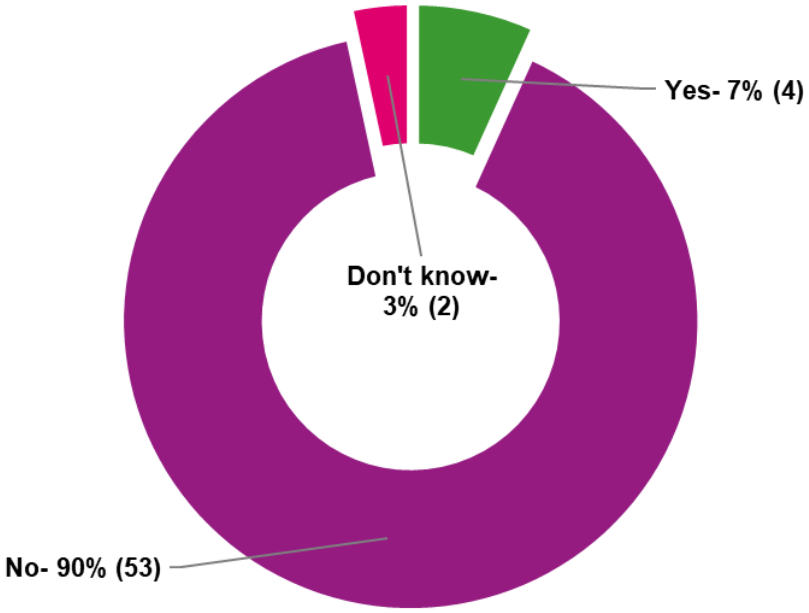
Base: Respondents who carry out tests and exercises of their cyber incident plans (29)

Cyber security arrangements

Just 7 per cent of respondent councils had experienced hostile cyber incidents over the last three years which led to unexpected costs or resourcing requirements. The majority (90 per cent) had not and the remaining three per cent did not know, as can be seen in Figure 24.

Those who had experienced an incident were asked to specify the costs and resourcing requirements associated with their incidents, however, due to the small numbers affected it has not been possible to produce statistically viable findings.

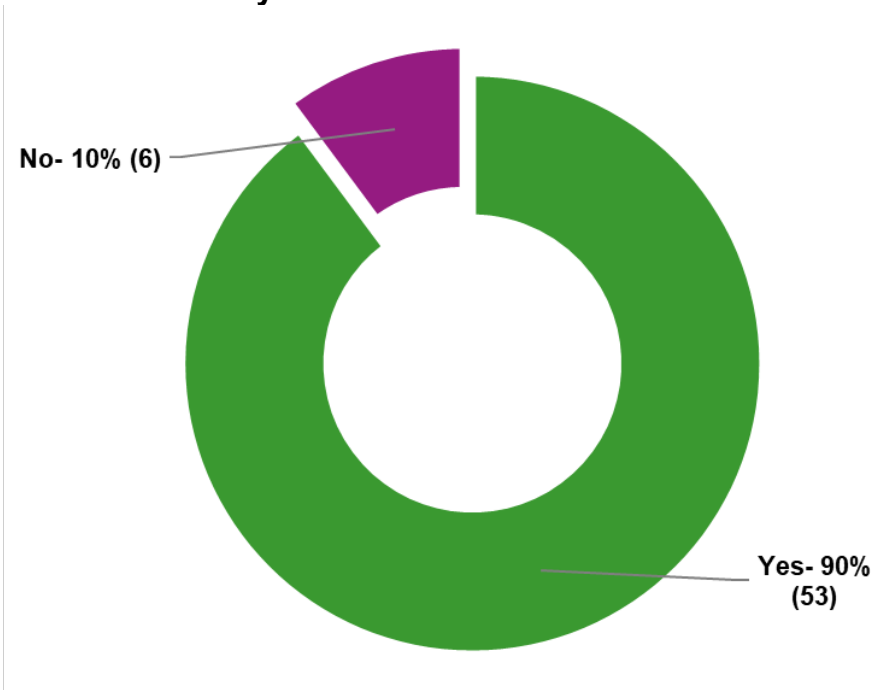
Figure 24: Has your council experienced any hostile cyber incidents over the last 3 years which led to unexpected costs or resourcing requirements?



Base: Respondents with cyber incident plans (56)

Most respondent councils (90 per cent) log, and bring together, security information from across their networks for analysis but one in ten (10 per cent) did not do this, as shown in Figure 25.

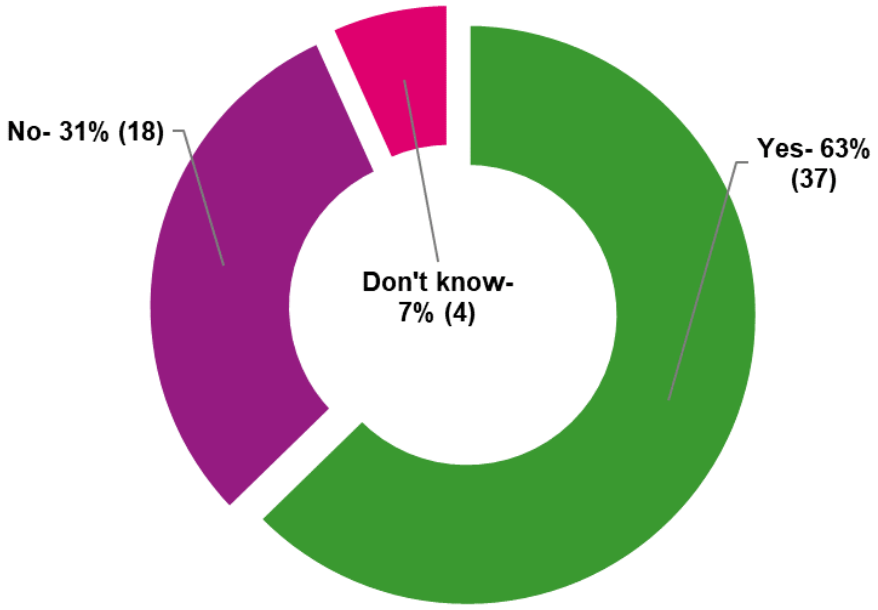
Figure 25: Does your council log, and bring together, security information from across its network for analysis?



Base: Respondents with cyber incident plans (56)

Almost two-thirds (63 per cent) of respondents reported having a Security Incident & Event Management solution (SIEM), 31 per cent did not have this and seven per cent did not know. These findings can be seen in Figure 26.

Figure 26: Does your council have a Security Incident & Event Management solution (SIEM)?

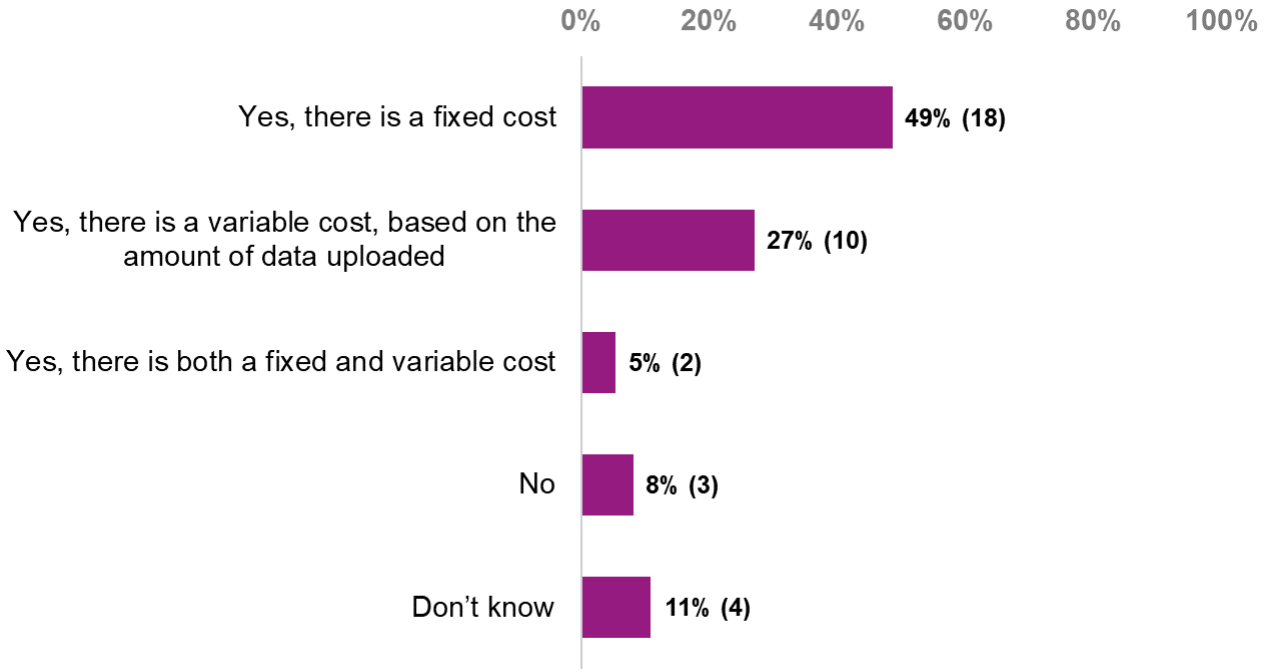


Base: Respondents with cyber incident plans (56)

Half (49 per cent) of respondents with a SIEM solution reported that they paid a fixed licensing cost for using it while 27 per cent paid a variable cost, based on the amount of data uploaded and five per cent paid both a fixed and variable cost. Just eight per cent of respondents did not have to pay to use their SIEM solution and ten per cent did not know if there was a licensing cost. Figure 27 illustrates these findings and a full breakdown is shown in Table 15.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 27: Is there a licensing cost to using this solution?



Base: Respondents with a Security Incident & Event Management solution (SIEM) (37)

Table 15: Is there a licensing cost to using this solution?

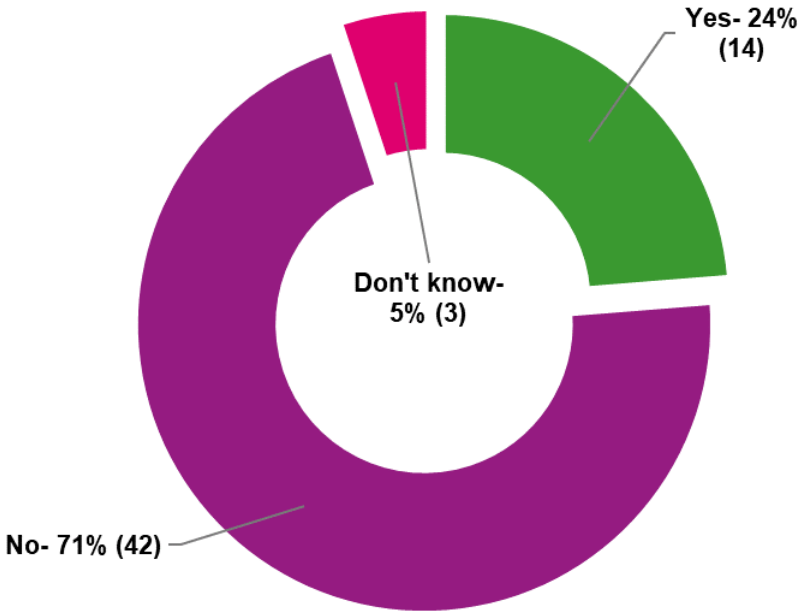
Answer	Number of responses	Per cent
Yes, there is a fixed cost	18	49%
Yes, there is a variable cost, based on the amount of data uploaded	10	27%
Yes, there is both a fixed and variable cost	2	5%
No	3	8%
Don't know	4	11%

Base: Respondents with a Security Incident & Event Management solution (SIEM) (37)

Respondents who paid to use their SIEM solution were asked about their licensing costs, however, due to the small number who answered this question it has not been possible to produce statistically viable findings.

A quarter (24 per cent) of respondents reported that they had a Security Operations Centre (SOC), 71 per cent did not and five per cent did not know if they had one, as shown in Figure 28.

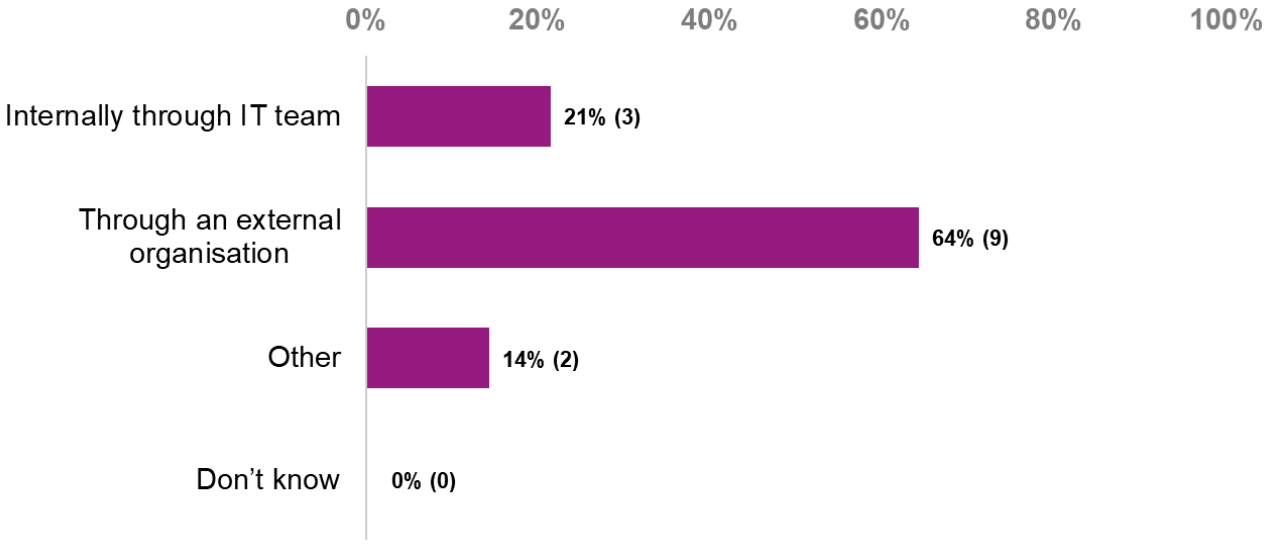
Figure 28: Does your council have a Security Operations Centre (SOC)?



Base: Respondents with cyber incident plans (56)

In almost two-thirds (64 per cent) of councils with a SOC it was delivered through an external organisation and in a fifth (21 per cent) it was delivered internally through the IT team. The remaining two councils (14 per cent) answered 'other', as they had more complex arrangements in place. Figure 29 illustrates these findings and the answers given by the councils using other ways to deliver their SOCs are shown in Table A17 in Annex A. As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 29: How is it delivered?

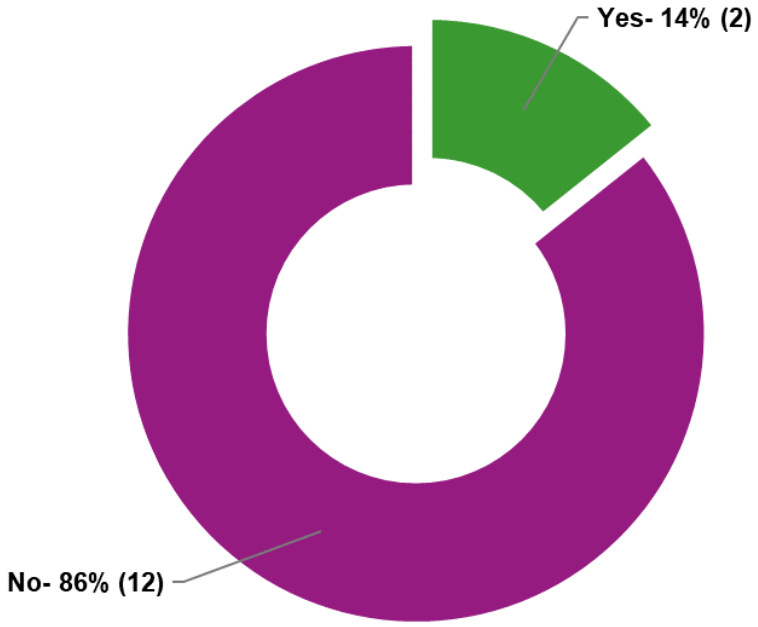


Base: Respondents with a Security Operations Centre (SOC) (14)

Just two (14 per cent) of the respondent councils with a SOC shared it with another council, as shown in Figure 30. One reported that there was a total of ten councils sharing in their SOC while the other reported their total as six. As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Respondents with a SOC were asked about their annual operating costs, however, due to the small number who answered this question it has not been possible to produce statistically viable findings.

Figure 30: Does your council share a SOC with any other organisations?

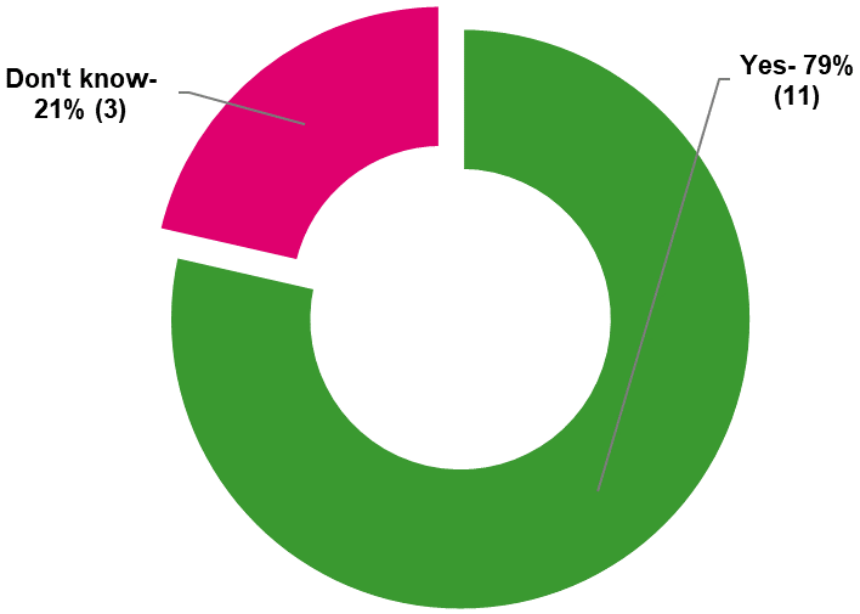


Base: Respondents with a Security Operations Centre (SOC) (14)

Most (79 per cent) of the respondents who had a SOC thought that cyber security at their council improved since its introduction, as can be seen in Figure 31. When they were asked to provide further details of the ways in which they thought cyber security had improved respondents most commonly mentioned monitoring. All of the answers provided are shown in Table A18 in Annex A.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 31: In your opinion, has cyber security at your council improved since the introduction of the SOC?

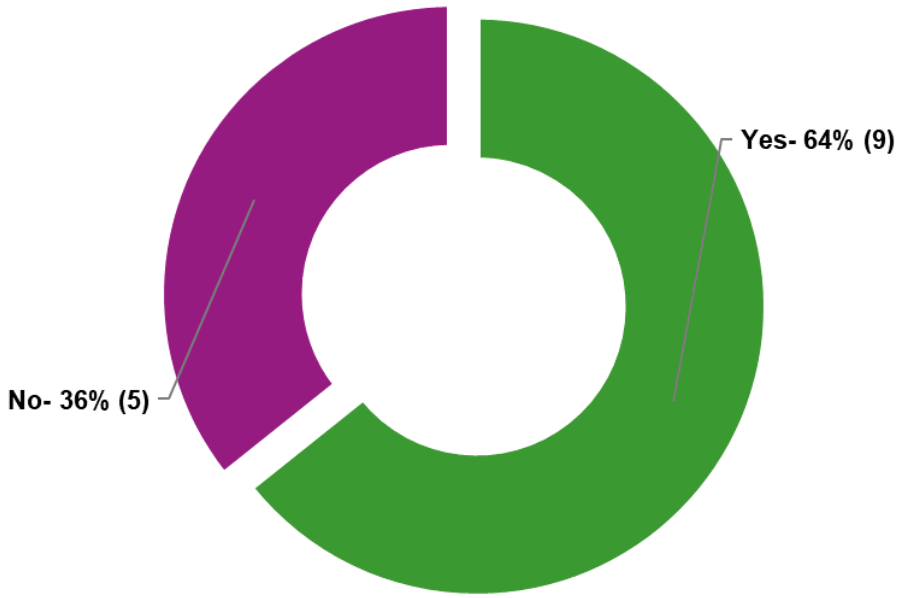


Base: Respondents with a Security Operations Centre (SOC) (14)

Among respondents with a SOC almost two-thirds (64 per cent) had 24-hour cover each day to deal with security incidents identified by its SOC, as shown in Figure 32. The 36 per cent who did not have 24-hour cover each day were asked to explain why not, their responses included costs and the scope of their contracts. A full list of the answers provided can be found in Table A19 in Annex A.

As there were only a very small number of respondents in this group, the findings should be treated with caution and cannot be seen as representative of all councils.

Figure 32: Does your council have 24-hour cover each day to deal with security incidents identified by its SOC?



Base: Respondents with a Security Operations Centre (SOC) (14)

The comments made by the respondents who provided further details about their council's cyber security arrangements included operational information about their SOCs, their cyber security resourcing levels and local cyber security arrangements. All of the answers provided can be seen in Table A20 in Annex A.

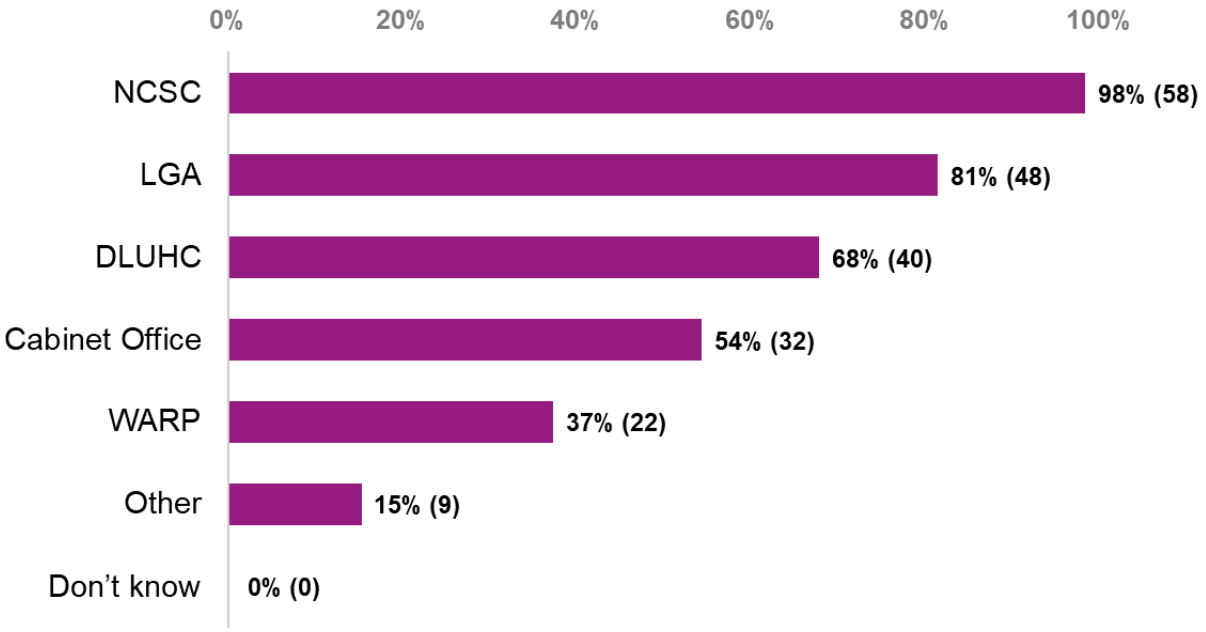
Information and Support

Almost all respondents (98 per cent) reported that they used NCSC as a source for guidance and support in relation to cyber security and their council's cyber incident response planning, 81 per cent used the LGA and 68 per cent used DLUHC.

Those who reported using other sources were asked to specify these, the answers provided included their suppliers, NIST and their LRF.

A full breakdown of these findings is shown in Figure 33 and is listed in Table 16. All the 'other' answers provided can be seen in Table A21 in Annex A.

Figure 33: Which sources of information, if any, do you currently use to access guidance and support in relation to cyber security and your council's cyber incident response planning?



Base: All respondents (59) Note: Respondents could select more than one answer

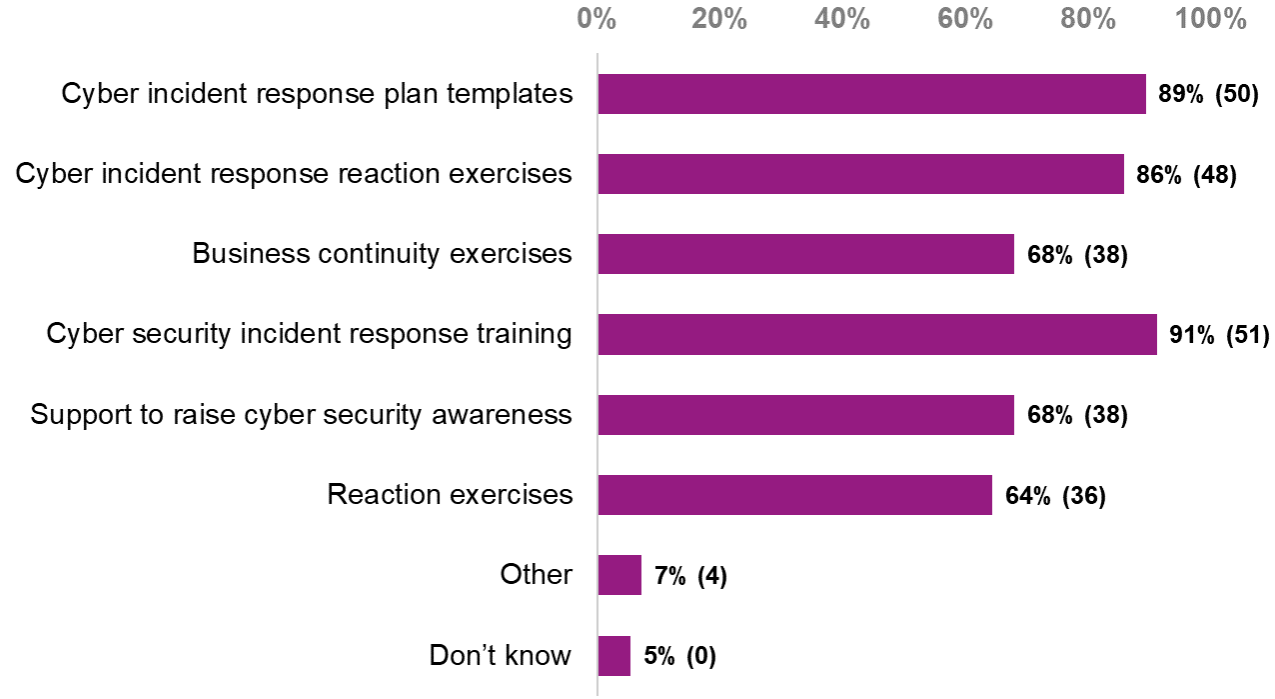
Table 16: Which sources of information, if any, do you currently use to access guidance and support in relation to cyber security and your council's cyber incident response planning?

Answer	Number of responses	Per cent
NCSC	58	98%
LGA	48	81%
DLUHC	40	68%
Cabinet Office	32	54%
WARP	22	37%
Other	9	15%
Don't know	0	0%

Base: All respondents (59) Note: Respondents could select more than one answer

When asked to select which, if any, cyber-related support they would like to receive from the LGA most respondents (86 per cent) selected cyber incident response plan templates. This was followed by cyber incident response reaction exercises (85 per cent) and cyber incident response reaction exercises (81 per cent). The respondents who answered other were asked to specify what they wanted, this included regional or national SOC development support and grant funding opportunities. A breakdown of these findings is shown in Figure 34 and is listed in Table 17. All the other answers provided can be seen in Table A22 in Annex A.

Figure 34: What cyber-related support, if any, would you like to receive from the LGA?



Base: All respondents (59) Note: Respondents could select more than one answer

Table 17: What cyber-related support, if any, would you like to receive from the LGA?

Answer	Number of responses	Per cent
Cyber incident response plan templates	50	89%
Cyber incident response reaction exercises	48	86%
Business continuity exercises	38	68%
Cyber security incident response training	51	91%
Support to raise cyber security awareness	38	68%
Reaction exercises	36	64%
Other	4	7%
Don't know	3	5%

Base: All respondents (59) Note: Respondents could select more than one answer

A very small number of respondents provided further comments about their council's information and support requirements, these included help to raise awareness of the importance of Cyber security with Councillors, support to improve relation to buy in of the Cyber Assessment Framework and a free to use centralised training package for local government. The answers provided can be read in full in Table A23 in Annex A.

Annex A

Answers provided to open text questions

Table A1: Which of the following most closely describes your council's cyber incident response plan/plans? Other answers provided.

Departmental BCPs, Major Incident Response Plan, Cyber Security Incident Response Plan, DR Plan
Partial incident runbook to be followed by technical team; needs to be completed
We are currently undergoing an exercise, with the LGA, to understand how senior leaders respond to a cyber incident and how they would invoke a series of departmental and organisational BCP's. It is hoped this will help to inform a wider piece of work around BCP gaps and disaster recovery planning

Table A2: Which of the following are included in your council's cyber incident communications strategy? Other answers provided.

Linkage into Corporate Communication teams
To be assessed depending on the incident

Table A3: If you would like to provide further details about your council's cyber incident communications strategy you may do so here: Comments received

Details of strategy
For minor incidents, the Digital Incident Management Team directly communicates with all staff members. However, for major occurrences, such as cyber incidents, this team liaises with the Response Group. This group consists of selected individuals responsible for activating other crucial protocols, including the Disaster Recovery and Business Continuity Plans.
In ICT both the Cyber Security Incident response plan and Disaster Recovery Plan will be invoked. Across the entire business, each service area will invoke their own BCP plans.
Status of strategy
I would say our cyber incident plans are very immature at this stage and would operate on a best endeavours basis. We are working with the LGA on a cyber incident to test senior leadership response which is hoped will feed into a wider programme of improvement in this space.
Our plan is currently being refreshed. We are using this survey to further inform the content of our refreshed plan so the timing of this survey is incredibly helpful.

Table A4: If you would like to provide further details about your council's cyber incident plan/plans you may do so here: Comments received.

Position of plans within wider emergency planning
Fundamentally the ICT Major Incident process and Disaster Recovery plan have been developed to include Cyber Security incidents. This includes recovery priorities as well as essential contacts and decision making trees.
Incident response is more geared towards DR scenario and covers only a subset of the systems in use.
Our Civil Resilience team will have software and solutions for crisis management.
Future development of plans
Business Continuity is something that we now have on our agenda and is something that is being further developed after a cyber exercise the authority has organised with consultants from <*company name*> in Oct/Nov 2023. They are organising a cyber event as well as reviewing the Business Continuity plans and potential issues with our senior leadership team
Following our Cyber 360 this is part of the action plan that we are taking forward
More needed to be done, BCPs need improvements and we need to test. We have plans to use the 'scenario in a box' from LGA in Q3 this year.
Recent insight will allow these plans to be further developed. A contact details App has been developed for all Civil Contingency\Emergency planning events.
Testing
<*Council name*> has an IT DR process that is tested with a 3rd party Business Continuity provider. This provider also manages all of <*Council name*>'s backups. We test our system recovery once a year.
We have dedicated cyber resource across a shared IT service with 2 other Councils. We have exercised with <*area name*> partners to test the Cyber Plan. More needed to be done, BCPs need improvements and we need to test. We have plans to use the 'scenario in a box' from LGA in Q3 this year.

Table A5: How was your council's cyber incident plan/plans developed? Other answers provided.

Both organically over time and in conjunction with supply chain discussion
Developed in partnership with <*company name*> the IT and Security MSP as part of procured service.
It was developed following the SANS Institute PICERL Methodology
Local IT Team
With support from the LGA

Table A6: To what extent was the council's senior management team involved in the development of its cyber incident plan/plans? Other answers provided.

Assistant Chief Executive (to a small extent)

Assistant Director Policy Strategy & Resources (to a small extent)
Chief Operating Officer (to a great extent)
Corporate Lead Infrastructure (to a great extent)
Director: Communities, Customer and Commercial Services (to a great extent)
Executive Director - Environment, Transport & Infrastructure (to a moderate extent)

Table A7: If you would like to provide further details about the development of your council's cyber incident plan/plans you may do so here: Comments received.

Development of plans
Created with Head of Apps & Systems, Enterprise Architect, Head of Information & DPO, Information Manager, Information Security Manager and Senior Information Security Officer other technical and non-technical IT leads. The plan will be reviewed and approved by Chief Digital Officer/SIRO.
Developed from NCSC guidance, other LAs plans and agreed with the senior management team
Plans developed in partnership with other <*council types*> who are in a shared ICT service. Gave robust resource that would not have been possible as a <*council type*> alone
The council has a Business Continuity and Emergency Planning Group which has a lead officer with established Business Continuity practices and plans for the council. The Cyber Incident Response Plan was developed with the Business Continuity and Emergency Planning Lead to dovetail with existing Business Continuity processes and plans.
The incident response (DR) plan was created several years ago and, I believe, was principally geared around maintaining "danger to life" systems.
Future development
CMT workshop is planned for October, to involve senior stakeholders in the plan.
Historically I would say to a small extent against each of the listed roles above. However, it is recognised this needs to change and we are actively engaged with the LGA to run a cyber incident scenario which will help to inform a wider strategy. I'm recently into post, as Strategic Cyber Security Manager, and so am keen to push the cyber incident and planning agenda with senior leaders. It currently sits at the top of our corporate risk register and so senior leaders are aware of the importance of planning.
The Cyber 360 peer review has an action plan which we are working through
Senior management team involvement
The Senior Management were not involved in the meetings for developing the Incident Response Plan but were invited to edit and comment accordingly.
We had a director / board level sponsor of the plan, exercises are to be planned.
Other

Business Continuity plans consider a prolonged outage of ICT services, ICT DR plan deals with recovery. Major Incident process allows for escalation of an ICT event such as a Cyber Security incident.
<*Council name*> has been outsourced to <*organisation name*> which would have covered cyber security. This contract ends next week at the end of Sept. <*Council name*> will be taking this over service from <*organisation name*> at the end of the contract. <*Council name*> doesn't have a deputy CEO
Playbooks and shared knowledge was also shared as part of <*Region name*> WARP

Table A8: How often, if at all, are the duties of the cyber incident response team tested by those undertaking them? Other answers provided.

Regular
Aim for every year however, this is not always possible due to resource constraints
Quarterly DR exercises
The plan is tested by using different playbooks (exercises in a box) which tests different scenarios and the overarching Incident Response Plan. Every month a different playbook is tested
We have a dry run of our technical DR processes every 3 months
We have various BC based scenario workshops each year. Cyber is usually once every couple
Ad hoc
Any data breach is treated as a cyber attack so incident response adopted until proved otherwise.
Depends, ICT regularly use the incident responses plans when we have a security incident, but this wouldn't be the same as a major attack such as a ransomware attack.
Duties are tested throughout the year on an ad hoc basis
Future
Not currently defined however will be in our refreshed plan.
We are planning internal exercises, previously this was external LRF exercise
Other
It used to be tested annually but has not been done for several years.
Not scheduled, we have tested with partners - need to do local testing
This is a new Cyber Incident Response for the council and only minimal testing has been done.

Table A9: If you would like to provide further details about your cyber incident response team, you may do so here: Comments received.

1st test will take place in Oct with <*company name*>

No major testing for our Cyber Incident Response Plan has taken place yet but hoping to carry this out soon.
Planned testing to be carried out after approval of cyber incident plans. Workshop scheduled to cover ransomware and phishing in November 2023.
Regarding point 12.,13. & 14. - whist the cyber incident response team and leadership have not been tested with a full cyber incident, they have been involved in multiple live business continuity scenarios.
Will endeavour to test 6 monthly going forward

Table A10: Who has received this training? (Cyber incident response training been provided to staff outside of the cyber incident response team)

A wide group of staff from Business Continuity, Estates, Comms, HR etc, in the form of exercises.
All Heads of Service
BC leads, and key contacts in services
Extended Leadership Team
Information Governance Group (director level board membership), Wider ICT Teams, Information Governance Team.
Tech teams
This is typically with the business continuity representatives through cyber-incident exercising.

Table A11: Which of the following, if any, apply to your council's backup system? Other answers provided.

Cloud based. Restorable and recoverable, with limited testing of the end-to end restoration process to identify potential recovery issues.
Cloud-hosted DR backup solution
Partially immutable, but all backed up offsite
We have a mix of 100% replication between DR, and backup that has tape capability.

Table A12: If you would like to provide further details about your council's preparations, you may do so here: Comments received.

Current status of progress
Discussions are ongoing around options to retain an organisation for cyber assurance support/expertise.
Testing of recovery from backups to be improved.
We are currently in a procurement exercise to procure a retainer.
We have been developing a relationship with <*company name*> to provide support/training and advice to our SLT and CEO

Work is underway to implement full 321 backup in line with NCSC recommendations as we recognize the current gap
Local arrangements in place
I'm not aware that NCSC provide an assured list of cyber incident response company's. We do however have a qualified supplier to provide the council with cyber security incident response and investigation services.
Retainer with <*company name*> for incident response support.

Table A13: How frequently is cyber incident testing and exercising undertaken? Other answers provided.

Currently done every other month on average
Done test with LRF, need to do local test
Every month, but this is not a full test, it will be playbooks. The intention is a full test which effectively replicates a full outage of the council's ICT services will take place at least annually. This hasn't been performed yet as the Incident Response Plan was developed this year so we are still testing it out through the use of playbooks such as phishing attacks, compromised user account credentials etc.
It isn't scheduled going forward, but we did an exercise this year
Randomly to reflect real-world - at least two a year
Try to perform tests annually.

Table A14: Which of the following scenarios have been covered in your council's cyber incident exercises and tests? Other answers provided.

BYOD, Supply chain security
Unknown Wi-Fi network, third party software compromise, BYOD

Table A15: Does your council use any of the following to conduct business continuity and/or cyber security exercises? Other answers provided.

NCSC exercises in a box (x 3)
<*Region name*> WARP events (x 2)
Backdoors and Breaches
LRF
<*Company name*> cyber simulations
Waiting on the new LGA BC exercise offering !!!!

Table A16: If you would like to provide further details about your council's cyber exercises and tests you may do so here: Answers provided.

External company delivered an exercise early 2023 to all members of ELT. LGA delivered an exercise early 2023 to ICT team. Planned to deliver ICT exercise later 2023. Planned to deliver exercise to include Comms and member of ELT early 2024

The council has a set of plans which are in progress/being updated in 2023 including the cyber incident response plan. We plan to run tests of our cyber incident plan, and have our DR plan externally validated to ensure it is fit for purpose. BC plans are created by each separate department and we plan to run an exercise in winter to cover BCP and loss of IT.
The council's cyber exercises and tests are in the planning phase. Over the past few years it has not been prioritised, but with a CISO appointed it is beginning to be taken more seriously and progress is starting on introducing exercises and testing.
There is a continual process of real life monitoring - detection and prevention that cover all of the above areas. It is planned for council wide Business Continuity exercises to take place within the next 12 months.
We were about to test but have recently suffered a real breach which has provided far greater insight than a trial run.
We're actively planning training and development, including test scenarios of cyber incidents

Table A17: How is [*your SOC*] delivered? Other answers provided.

Internal SOC Team working alongside Security HQ providing analysis and event monitoring
We have both an internal SOC and an external SOC. The external SOC manage our instance of our SIEM and the incidents generated.

Table A18: Please provide further details of the ways in which you think cyber security has improved. Answers provided.

Monitoring
24/7 Monitoring with autonomy to isolate and threat hunting
Event monitoring is active, in place and maturing. The SOC has identified and dealt with incidents arising from this monitoring
Improved monitoring, early detection, playbooks acted upon
Other answers
General awareness across the organisation; plans; scenarios; reporting
Information sharing has improved to help identify weaknesses.
Specialist experts
The SOC is delivered as part of our ICT managed services contract , security is just one change delivered as part of this contract and features heavily within the design and delivery of all BAU services
We have undertaken a huge improvement in Cyber Security over the past few years. We have an CISSP Qualified Network Support Leader, Rationalised Security - Implemented <*Product name*> throughout entire estate, implemented <*Product name*>, Implemented a 24 hour External SOC, <*Product name*>, MFA on RDP, Least Privilege review, On Prem PAM, Undertaken DLUHC Cyber Treatment Plan, Engaged with DLUHC on Cyber Assessment Framework Pilot - taking value

from that to work towards Cyber Assessment Framework compliance, General Security improvements within IT "Security by Design" and changing whole ethos re approach to security - it is there to protect our ability to deliver statutory services & our customers data - not be seen as a barrier or hinderance.
Whilst I have alluded to the fact that our cyber response plans are immature, we have embarked on work that has seen some marked improvements, not least the appointment of an external SOC to manage incidents via our SIEM and respond on our behalf. We have also seen head count increase within our internal team.

Table A19: Please explain why 24/7 coverage is not provided to deal with security incidents identified by your council's SOC: Answers provided.

Cost related reasons
Business decision on cost.
No budget for 24/7 staffing
Contract related reasons
Not documented specifically - it is in contracts. Staff are on-call but not necessarily "ready"
This was not included in the scope of the existing contract, something we are looking to change when the contract comes up for renewal
Other reasons
The SOC is 24/7 but Council resource isn't

Table A20: If you would like to provide further details about your council's cyber security arrangements you may do so here: Answers provided.

SOC related answers
24 hour cover is provided by <*company name*>. They in turn have out of hours contact details for key <*council name*> staff and a route into internal SOC to trigger coordination of a response.
24 hour SOC - engagement several times a week - and monthly reviews - lessons learned. The team now live and breathe security with it embedded with software development, desktops and networks - security by design and security first.
One is under creation
Progressing business case to gain approval to implement a 3rd party SOC.
The SOC is currently being implemented, it is not fully operational yet, it should be live this calendar year. It was procured through Integrated Care Board partners (so <*council names*> and various health organisations). Light housing is used to allow the 3rd party SOC provider to access the <*company name*> SIEM logs.
We have a hosted SOC
We have a Service Operation Centre 24/7/365 which would manage this service through our MSP Agreement. As part of that a Security Operation Centre has just gone live through <*company name*>.

We haven't yet gone live with the SOC so we are unable to provide an opinion on whether cyber security has been improved, but we anticipate that the SOC will provide added cyber security resilience once implemented this winter.
Local cyber security arrangements
Depends what you class as a SOC. We have staff trained in assisting with cyber security, running regular monthly scans and updating / reporting on systems issues, so in some ways yes. The issue for us is out of hours SOC, we do not have out of hours cover, we have looked at procurement of this and it has been cost prohibitive. A national SOC which councils could buy into would be beneficial to provide out of hours SOC.
No formal SOC but internal IT team have roles defined within the service BCP that support DR procedures. Internal IT BCP team procedures are aligned with senior management control activities in the event of an incident.
We have a general Security Team whose duties include monitoring security events as they arise but they are not a team dedicated to SOC operations only.
We have an inhouse IT provision, we work closely with our regional peers via the WARP or CISP, or other channels via Slack.
Resourcing
2 x FTE ITSEC Officers
24 hour cover is available via our on-call staff member
A Cyber and Information Security Officer has been hired in within the last 6 months, which is the main individual in the organisation that is allocated roles and responsibilities related to security of the network and systems.
<*Council name*> is a very small authority with <*number*> staff
Other
At the end of last year, we were fortunate to receive a grant from the DLUHC to help improve our cyber security standing. As part of the work coming out of this we are engaging with external experts on creating and promoting a cyber incident plan across the authority (especially senior managers). We are also just about to start a proof of concept, with <*company name*>, of <*product name*>, their SIEM. This is due to run until the end of October and will provide valuable training into the use of a SIEM and also understand the amounts of data that need to be ingested and the likely ongoing costs of a SIEM solution.
SIEM is proving difficult to source. We're going to look at <*product name*> - as a new version has now been released.

Table A21: Which sources of information, if any, do you currently use to access guidance and support in relation to cyber security and your council's cyber incident response planning? Other answers provided.

Commercial organisations (x 3)
Existing suppliers (x 2)
LRF (x 2)
NIST (x 2)

Colleagues
<*Council name*> Civil Contingency Unit
NHS
NISC
Other council
UK Gov Digital Slack

Table A22: What cyber-related support, if any, would you like to receive from the LGA? Other answers provided.

Anything else that is available.
Centralised/Regional SOC for Local Government.
If there is the opportunity to bid for funding to strengthen our overall incident response posture that would be greatly received.
Regional or National SOC development support

Table A23: If you would like to provide any further comments about your council's information and support requirements, you may do so here: Answers provided.

All of the above would be useful. Could there not be a centralised training package which was free for use for all staff that all local government could access, I'm sure it would be cheaper to do this nationally, rather than us all have to procure or develop our own.
Cyber security is something that continually evolves. We would welcome any support offered to help us improve our cyber security posture - particularly would welcome member / SLT presentation / training to ensure wide buy in of the Cyber Assessment Framework (CAF). By full engagement of the CAF and support of it (including the rationale behind IT Security resource) we will considerably increase our cyber security posture and lower our risk of cyber attack.
Support from LGA to help raise awareness of the importance of cyber security with councillors as they are one of our most common targets for example phishing emails due to their position.

Annex B

Survey Questionnaire

Response and Recovery Survey 2023

The purpose of this survey is to build a better understanding of how prepared the local government sector is to respond to a cyber incident. This will enable the LGA to shape it's Cyber, Digital and Technology programme and ensure that councils have the support they most need to respond to the increasing cyber threat.

You can navigate through the questions using the buttons at the bottom of each page. Use the 'previous' button at the bottom of the page if you wish to amend your response to an earlier question.

Please note, you will be routed through the survey on the basis of the answers you provide and therefore may not see all of the questions. If you would like to see how the routing directs respondents please refer to the PDF version of the survey, which can be accessed below.

If you stop before completing the return, you can come back to this page using the link supplied in the email and you will be able to continue where you left off. To ensure your answers have been saved, click on the 'next' button at the bottom of the page that you were working on before exiting.

All responses will be treated confidentially. Information will be aggregated, and no individual or authority will be identified in any publications without your consent. Identifiable information may be used internally within the LGA and DLUHC (with personal information removed) but will only be held and processed in accordance with our privacy statement. We are undertaking this survey to aid the legitimate interests of the LGA in supporting and representing authorities.

If you would like to see an overview of the questions before completing the survey online, you can access a PDF here: <*link to PDF*>

Please amend the details we have on record if necessary.

If you are responding on behalf of more than one council please ensure this is shown in the 'council' box below.

Name _____

Council _____

Job title _____

Email address _____

Cyber incident response planning

1. Does your council have a plan, or plans, to help it respond and recover in the event of a cyber incident?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q2, if no go to Q28

2. Which of the following most closely describes your council's cyber incident response plan/plans?
Please select all that apply

- ❑ An organisation wide cyber incident response plan
- ❑ An organisation wide business continuity plan (BCP)
- ❑ A critical services BCP
- ❑ An IT prioritised recovery plan/BCP
- ❑ Departmental/Service wide IT disaster recovery plan
- ❑ A plan that feeds into a Local Resilience Forum cyber incident response plan
- ❑ Other (please specify below)

  _____
- ❑ Don't know

3. Which of the following are included in your council's cyber incident plan/plans?
Please select all that apply

- ❑ A named incident response team
- ❑ Defined roles and responsibilities
- ❑ Decision-making protocols
- ❑ Response escalation criteria
- ❑ Playbooks for different scenarios
- ❑ Legal and regulatory requirements
- ❑ Communications strategy
- ❑ Protracted total loss of IT
- ❑ Loss of access to data
- ❑ Backup restoration times
- ❑ Post incident review
- ❑ Stand down process
- ❑ Other (please specify)

  _____
- ❑ Don't know

If there is a comms strategy go to Q3a, if not go to Q4

3a. Which of the following are included in your council's cyber incident communications strategy?
Please select all that apply

- ❑ Channels to communicate with staff in the event of a total loss of IT
- ❑ Internal communications principles
- ❑ Customer/resident communications principles
- ❑ Supplier/business partner communications principles
- ❑ Media statements and materials
- ❑ Other (please specify below)

  _____
- ❑ Don't know

3b. If you would like to provide further details about your council's cyber incident communications strategy you may do so here:

_____

_____

4. Would your council's cyber incident plan/plans be accessible if there was a total loss of IT?

- ❍ Yes
- ❍ No
- ❍ Don't know

5. Would contact details for key personnel who will handle the response to an incident be accessible if there was a total loss of IT?

- ❍ Yes
- ❍ No
- ❍ Don't know

6. Does your council use bespoke/third-party software to support business continuity management?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q6a, if no got to Q7

6a. Who provides the software for your council's business continuity management?
[*These findings are not reported due to commercial interests - s43(2) FOIA 2000*]

_____

7. If you would like to provide further details about your council's cyber incident plan/plans you may do so here:

_____

_____

8. How was your council's cyber incident plan/plans developed?

- ❍ Organically over time
- ❍ Strategically based on identified/potential risks
- ❍ Other (please specify below)

  _____
- ❍ Don't know

9. Did any of the following inform the development of council's cyber incident plan/plans?

- ❑ A cyber incident at your council
- ❑ A cyber incident at another council/organisation
- ❑ Cyber incident exercises and testing
- ❑ Changes in legislation and national guidance
- ❑ Don't know

10. To what extent was the council's senior management team involved in the development of its cyber incident plan/plans?
Please align your council's job titles with the nearest general role shown or, if that is not possible, use the 'other' category.

	To a great extent	To a moderate extent	To a small extent	Not at all	Don't know
Chief Executive	○	○	○	○	○
Deputy Chief Executive	○	○	○	○	○
Director of Corporate Services (incl. Finance)	○	○	○	○	○
Director of Finance	○	○	○	○	○
Director of Corporate Services (without Finance)	○	○	○	○	○
Chair of Information Governance Board/Senior Information Risk Owner (SIRO)	○	○	○	○	○
Other (please specify) _____	○	○	○	○	○
Other (please specify) _____	○	○	○	○	○

11. If you would like to provide further details about the development of your council's cyber incident plan/plans you may do so here:

_____

Incident response

12. Are the duties of the cyber incident response team explained to those undertaking them?

- ❍ Yes
- ❍ No
- ❍ Don't know

13. Has training been provided in the duties of the cyber incident response team?

- ❍ Yes
- ❍ No
- ❍ Don't know

14. How often, if at all, are the duties of the cyber incident response team tested by those undertaking them?

- ❍ Every six months
- ❍ Every year
- ❍ Every two years
- ❍ Other (please specify below)

  _____
- ❍ Duties have not been tested
- ❍ Don't know

15. If you would like to provide further details about your cyber incident response team, you may do so here:

_____

16. Has cyber incident response training been provided to staff outside of the cyber incident response team?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q16a, if no got to Q17

16a. Who has received this training?

_____

17. Which of the following, if any, apply to your council's backup system?
Please select all that apply

- ❍ Multiple copies with one offline/cold or immutable copy
- ❍ Held on at least two devices, with one offsite or offline
- ❍ Created frequently
- ❍ Restorable and recoverable, with full testing of the end-to-end restoration process to identify potential recovery issues
- ❍ Unauthorised access prevention
- ❍ Other (please specify below)

  _____

- ❍ Don't know

18. Does your council have arrangements in place to bring in external support, such as an NCSC assured cyber incident response company, if required?

- ❍ Yes
- ❍ No
- ❍ Don't know

19. If you would like to provide further details about your council's preparations, you may do so here:

_____

20. Does your council carry out tests and exercises of its cyber incident plan/plans?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q21, if no got to Q28

21. How frequently is cyber incident testing and exercising undertaken?

- ❍ Every three months
- ❍ Every six months
- ❍ Every year
- ❍ Every two years
- ❍ Other (please specify below)

  _____

- ❍ Don't know

22. Which of the following scenarios have been covered in your council's cyber incident exercises and tests?
Please select all that apply

- ❑ Phishing
- ❑ Data breach/exfiltration
- ❑ Suspicious account activity
- ❑ Ransomware
- ❑ Denial-of-service
- ❑ Other (please specify below)

  _____
- ❑ Don't know

23. Who is involved in your council's cyber incident exercises and tests?
Please select all that apply

- ❑ Cyber incident response team
- ❑ Emergency planning team
- ❑ Business continuity team
- ❑ IT Team
- ❑ Senior Management Team
- ❑ Heads of Service
- ❑ Chief Executive
- ❑ Chair of Information Governance Board/Senior Information Risk Owner (SIRO)
- ❑ Other (please specify below)

  _____
- ❑ Don't know

24. Which parts of the cyber incident response cycle are covered by your council's exercises and tests?
Please select all that apply

- ❑ Preparation
- ❑ Detection and analysis
- ❑ Containment, eradication and recovery
- ❑ Post-incident activity, including impact management
- ❑ Other (please specify below)

  _____
- ❑ Don't know

25. Does your council use any of the following to conduct business continuity and/or cyber security exercises?
Please select all that apply

- ❑ Bespoke software

- ❑ A subscription with an external organisation
- ❑ Other (please specify below)

  _____

- ❑ No
- ❑ Don't know

If using bespoke software or subscription go to Q25a, if no go to Q26

25a. Please provide the name of your council's bespoke software provider/subscription provider? [*These findings are not reported due to commercial interests - s43(2) FOIA 2000*]

_____

26. Are the lessons learnt from exercises and tests used to update your council's cyber incident plan/plans?

- ❍ Yes
- ❍ No
- ❍ Don't know

27. If you would like to provide further details about your council's cyber exercises and tests you may do so here:

_____

_____

Cyber security arrangements

28. Has your council experienced any hostile cyber incidents over the last 3 years which led to unexpected costs or resourcing requirements?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q28a, if no go to Q29

28a. What costs/resourcing requirements were associated with this incident from its beginning to its agreed end (incident closure)?
If you do not know the actual amounts please provide an estimate where possible

Unexpected costs could include the following:

- Activation of an existing incident response retainer
- External subject matter expertise
- Legal costs including legal counsel

- Procurement of new IT systems or Managed Security Service Provider contracts to harden networks
- Remediation and replacement of IT systems and hardware
- Reputation management
- Data breach response activities and data governance resourcing
- Staff overtime
- Loss of revenue during operational downtime
- Contract breaches and compensation
- Regulatory fines

		Are these figures:		
		Known costs/ resources	Best estimate	Unavailable
Unexpected costs (£)	_____	○	○	○
IT Team resources (days)	_____	○	○	○
Affected team(s) resources (days)	_____	○	○	○
Other team(s) (days)	_____	○	○	○

28b. If you would like to provide further details about your council's unexpected costs or resourcing requirements you may do so here:

_____

_____

29. Does your council log, and bring together, security information from across its network for analysis?

- ❍ Yes
- ❍ No
- ❍ Don't know

30. Does your council have a Security Incident & Event Management solution (SIEM)?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q30a, if no go to Q31

30a. Which SIEM solution is used?
[*These findings are not reported due to commercial interests - s43(2) FOIA 2000*]

- ❍ Microsoft
- ❍ Splunk
- ❍ LogRhythm
- ❍ Alienvault (AT&T)
- ❍ Security Onion
- ❍ Other (please specify below)

  _____

- ❍ Don't know

30b. Is there a licensing cost to using this solution?
Please select all that apply

- ❑ Yes, there is a fixed cost
- ❑ Yes, there is a variable cost, based on the amount of data uploaded
- ❑ No
- ❑ Don't know

If there are costs go to Q30c, if no go to Q31

30c. What are these costs?

		Are these figures			
		Actual cost	Best estimate	Unavailable	Cost not applicable
Fixed cost (£ p.a.)	_____	○	○	○	○
Variable cost (£ p.a.)	_____	○	○	○	○

31. Does your council have a Security Operations Centre (SOC)?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes *go to Q31a, if no go to Q32*

31a. How is it delivered?

- ❍ Internally through IT team
- ❍ Through an external organisation
- ❍ Other (please specify below)

  _____

- ❍ Don't know

31b. Does your council share a SOC with any other organisations?

- ❍ Yes
- ❍ No
- ❍ Don't know

31c. How many organisations share this SOC, including your council?

_____

31d. If your council's SOC is delivered through an external organisation, what are the annual operating costs?

		Are these figures:		
		Actual cost	Best estimate	Unavailable
£ p.a.	_____	○	○	○

31e. In your opinion, has cyber security at your council improved since the introduction of the SOC?

- ❍ Yes
- ❍ No
- ❍ Don't know

If yes go to Q31e(i), if no go to Q31f

31e(i). Please provide further details of the ways in which you think cyber security has improved.

_____

If yes go to Q31f(i), if no go to Q32

31f. Does your council have 24-hour cover each day to deal with security incidents identified by its SOC?

- ❍ Yes
- ❍ No
- ❍ Don't know

31f(i). Please explain why 24/7 coverage is not provided to deal with security incidents identified by your council's SOC:

_____

32. If you would like to provide further details about your council's cyber security arrangements you may do so here:

_____

Information and Support

33. Which sources of information, if any, do you currently use to access guidance and support in relation to cyber security and your council's cyber incident response planning?
Please select all that apply

- ❑ NCSC
- ❑ LGA
- ❑ DLUHC
- ❑ Cabinet Office
- ❑ Other (please specify below)

  _____
- ❑ Don't know

34. What cyber-related support, if any, would you like to receive from the LGA?
Please select all that apply

- ❑ Cyber incident response plan templates
- ❑ Cyber incident response reaction exercises
- ❑ Business continuity exercises
- ❑ Cyber security incident response training
- ❑ Support to raise cyber security awareness
- ❑ Reaction exercises
- ❑ Other (please specify below)

  _____
- ❑ Don't know

35. If you would like to provide any further comments about your council's information and support requirements, you may do so here:

_____

36. Would you be happy for us to contact to discuss the answers you have provided in relation to business continuity and/or cyber security exercises?

- ❍ Yes
- ❍ No

If yes go to Q36a, if no go to Q37

36a. Please provide details for how you would prefer to be contacted:

Phone number _____

Email address _____

37. If you have any further comments you would like to provide you may do so here:

_____

Once you press the 'Submit' button below, you will have completed the survey.

Many thanks for taking the time to complete this survey. You are in control of any personal data that you have provided to us in your response. You can contact us at all times to have your information changed or deleted. You can find our full privacy policy here: click here to see our privacy policy

Local Government Association
Local Government House
Smith Square
London SW1P 3HZ

Telephone 020 7664 3000
Fax 020 7664 3030
Email info@local.gov.uk
www.local.gov.uk

For a copy in Braille, larger print or audio, please contact us on 020 7664 3000.

We consider requests on an individual basis.