Assessing the cost of a cyber security breach

Draft costing tool

Ipsos MORI

How this tool works

We are developing a tool for the Department for Digital, Culture, Media and Sport to help organisations better understand the full extent of the costs they might incur from cyber security breaches. This is a version of that tool for testing.

The final version of this tool may be useful for organisations like yours to think about all the potential costs and impacts that a cyber security breach could have had. It may also be useful to insurance companies or external cyber security providers when trying to understand their clients' cyber security breaches.

How to use this tool

We know this is a long document. **You will <u>not</u> need to read all of it or fill it all in.** There are seven sections. The first section will give you an idea of the remaining sections to look at.

- Everyone fills in the first section. This is only 3 pages and takes 5-10 minutes. You may need to talk to other people in your organisation to answer fully.
- You may then need to read through up to four or five of the other sections and try to fill them in as much as you reasonably can.
- **We don't need you to be 100% certain of your answers.** We just want you to try and be as accurate and detailed as you can reasonably be. We will then use our interview with you to understand how you arrived at your answers and the challenges you faced.
- If you would prefer not to answer any questions, that is fine, but we would like to ask about the reasons why in the interview.
- **We will treat all your answers as confidential.** The answers are to help us test the tool, rather than to produce statistical data (about your or any organisation).

What will we ask you about in the interview?

In the interview, we will ask you about your experience of using this document and try to understand the thought process behind the answers that you write in here. This includes:

- how easy or difficult different questions were to answer
- how clear and distinct each of our categories and questions were
- who you had to talk to (or might have to talk to) within your organisation to get as accurate an answer as possible
- whether the questions made you think differently about the kinds of costs associated with cyber security breaches
- how the tool might help organisations to think about the cost of cyber security breaches.

1 The nature of the breach

Everyone fills in this section. Just write in or circle your answers throughout.

We would like you to **think about a cyber security attack, breach or incident that has had a disruptive impact on your organisation within the past 2 or so years**. The attack may not have been successful but could still have caused disruption (e.g. if there was work undertaken to stop it from getting past your cyber security defences).

This could be the disruptive breach you discussed with us in the telephone survey in winter 2019. It could be another breach that was more disruptive. We just want you to choose a scenario that allows you to fill in a few different sections in this document if possible.

1.1 Give us a brief description of this attack, breach or incident

1.2 Did any of the following happen? Tick all that apply.

For these categories, you may need to talk to **someone in your finance team**.

Category	Tick for yes	Sections from the rest of the document to answer
Money or other financial assets stolen (e.g. through illegitimate bank transfers)	☐	Answer 2.1 (pg. 5)
Staff stopped from carrying out their day-to-day work	☐	Answer 2.2 (pg. 5)
Paid a cyber ransom or any other payments to the perpetrators of the breach, in order to retrieve access to services	☐	Answer 2.3 (pg. 5)
The breach interrupted any of the normal services you provide (e.g. access to your website) – this is different to you choosing to shut down these services voluntarily	☐	Answer 2.4 (pg. 6)
Data or software lost, corrupted or encrypted	☐	Answer 2.5 (pg. 7)
Lost intellectual property (defined in our footnote)[1]	☐	Answer 2.6 (pg. 9)
Lost commercially sensitive information other than intellectual property (defined in our footnote)[2]	☐	Answer 2.7 (pg. 10)
IT equipment was damaged	☐	Answer 2.8 (pg. 11)
Other physical equipment damage (not including IT equipment)	☐	Answer 2.9 (pg. 13)
Paid an insurance excess	☐	Answer 2.10 (pg. 16)

[1] Intellectual property is a product of the intellect that has commercial value, including copyrighted or patented property such as literary or artistic works, appellation of origins, business methods, and industrial processes.

[2] This includes all commercially sensitive information that is not the subject of patents, copyright, design rights or trademarks, such as meeting notes, contractual agreements, negotiating strategies etc.

1.3 Did any of the following happen? Tick all that apply.

For the next categories, you may need to talk to **someone in a legal or compliance role**, such as a Data Protection Officer, or anyone else that deals with industry regulators.

Category	Tick for yes	Sections from the rest of the document to answer
Fines by regulators or authorities	☐	Answer 3.1 (pg. 17)
Legal action by those impacted by the breach	☐	Answer 3.2 (pg. 17)
You had to notify the authorities (e.g. police or a regulator)	☐	Answer 3.3 (pg. 18)
You had to notify customers, investors, suppliers or any other people or organisations you work with	☐	Answer 3.4 (pg. 19)

1.4 Did any of the following happen? Tick all that apply.

For the next categories, you may need to talk to **someone in a technical cyber security role** in your organisation (e.g. within your IT team).

Category	Tick for yes	Sections from the rest of the document to answer
You chose to shut down at-risk services (e.g. software applications or networks) to prevent further exposure to the breach	☐	Answer 4.1 (pg. 20)
Existing staff had to work overtime to resolve the breach	☐	Answer 4.2 (pg. 22)
You had to hire additional staff or engage an external cyber security provider or consultant on a temporary basis to help resolve the breach – this is different to long-term staff hires or long-term changes to cyber security practices	☐	Answer 4.3 (pg. 23)
You spent time investigating the source of the breach	☐	Answer 4.4 (pg. 23)
Provided additional cyber security protection to customers, investors, suppliers or any other people or organisations you work with	☐	Answer 4.5 (pg. 24)
Changed any internal IT or cyber security policies, technical controls, processes or providers (e.g. internet service providers or software providers)	☐	Answer 4.6 (pg. 25)
Hired new staff, permanently increased hours of existing staff or engaged external cyber security providers on a permanent basis, or carried out more staff training on cyber security	☐	Answer 4.7 (pg. 27)

The final question in this section is on the next page.

1.5 Did any of the following happen? Tick all that apply.

For the next categories, you may need to **someone in your senior management team**.

Category	Tick for yes	Sections from the rest of the document to answer
You provided compensation (e.g. money or vouchers) to the customers, investors, suppliers or any other people or organisations you work with	☐	Answer 5.1 (pg. 30)
You provided discounts to customers	☐	Answer 5.2 (pg. 30)
You had to deal with complaints (e.g. from those impacted by the breach)	☐	Answer 5.3 (pg. 30)
Engaged in PR or marketing activities in response to the breach (e.g. on social media, advertising or any other communications)	☐	Answer 5.4 (pg. 32)
A reduction in investment or donor funding	☐	Answer 5.5 (pg. 33)
You decided to reduce spending on research and development or investing in a new production process or technology as a direct result of the breach – this is different from lost research and development linked to loss of intellectual property	☐	Answer 5.6 (pg. 34)
Downgrading of credit rating	☐	Answer 5.7 (pg. 34)
Increase in any insurance premiums	☐	Answer 5.8 (pg. 35)
Increased difficulty in recruiting new staff	☐	Answer 5.9 (pg. 35)
You lost customers	☐	Answer 5.10 (pg. 36)
You lost suppliers	☐	Answer 5.11 (pg. 36)

2 Immediate losses or damage

For these questions, you may need to talk to **someone in your finance team**.

2.1 If money or other financial assets stolen (e.g. through illegitimate bank transfers)

a. What was the quantity of money/financial assets lost?

– £

2.2 Staff stopped from carrying out their day-to-day work

a. How many staff were prevented from carrying out their day-to-day work?

–

b. For how long was each staff member/staff band prevented from carrying out their day-to-day work? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

c. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those prevented from carrying out their work? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

2.3 Paid a cyber ransom or any other payments to the perpetrators of the breach, in order to retrieve access to services

a. What was the value of the payment made?

– £

2.4 The breach interrupted any of the normal services you provide (e.g. access to your website)

a. Which services were unavailable? Select all that apply.

- Email
- Internal communication systems
- External client facing systems (e.g. marketing, purchasing)
- Internal systems (e.g. HR)
- Website
- Other (please state)
- [ ]

b. For each service selected above, was the service partially or completely unavailable?

- Completely unavailable
- Partially unavailable

c. For each service selected above, if partially unavailable, to what extent was the service unavailable (where 100% is completely unavailable)?

- [ ] %

d. For each service selected above, if unable to provide percentage, was it:

- Less than 20% unavailable
- 20%-40% unavailable
- 41%-60% unavailable
- 61%-80% unavailable
- More than 80% unavailable

e. For each service selected above, what was the duration of time for which the service was unavailable?

- [ ] hours/days (select as appropriate)

f. For each service selected above, if unable to provide percentage, was it:

- Less than an hour
- Between an hour and a day
- 1-3 days
- 4-5 days
- 6-10 days
- More than 10 days

g. For each service selected above, is the service directly related to revenue generation?

- Yes
- No

h. If yes, for each service selected above, through which mechanism was revenue affected? Please give a brief description.

–

i. For each service selected above, what is the amount of revenue associated with the service per hour/day/month (select as appropriate)?

– £

j. For each service selected above, if unable to provide a figure, was the estimated revenue loss per day as a result of the interruption to the service:

- Less than £100
- Between £100 and £200
- £201 to £500
- £501 to £1,000
- More than £1,000

2.5 Data or software lost, corrupted or encrypted

a. Did the loss/corruption or encryption of data result in disruption in service provision?

- Yes
- No

b. If yes, which service was unavailable? Select all that apply.

- Email
- Internal communication system
- External client facing systems (e.g. marketing, purchasing)
- Internal systems (e.g. HR)
- Website
- Other (please state)

–

c. For each service selected above, what was the duration of time for which the service was unavailable?

– hours/days (select as appropriate)

d. For each service selected above, if unable to provide percentage, was it:

- Less than an hour
- Between an hour and a day
- 1-3 days
- 4-5 days
- 6-10 days
- More than 10 days

e. For each service selected above, is the service directly related to revenue generation?

- Yes
- No

f. If yes, for each service selected above, through which mechanism was revenue affected? Please give a brief description.

-

g. For each service selected above, what is the amount of revenue associated with the service per hour/day/month (select as appropriate)?

- £

h. For each service selected above, if unable to provide a figure, was the estimated revenue loss per day as a result of the interruption to the service:

- Less than £100
- Between £100 and £200
- £201 to £500
- £501 to £1,000
- More than £1,000

i. Was staff time required to resolve the loss/corruption or encryption of data

- Yes
- No

j. How many staff were required to resolve the loss/corruption or encryption of data?

-

k. How long was each staff member resolving the loss/corruption or encryption of data? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

l. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those resolving the loss/corruption or encryption of data? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

2.6 Lost intellectual property

a. Has the loss of intellectual property resulted in the firm losing competitive advantage?

- Yes
- No

b. If yes, how did your firm determine the loss of competitive advantage?

- Emergence of new competition
- Appearance of copied products or activities
- Soured deals or business ventures
- Compromised negotiations
- Other (please state)
-

c. What was the value of the intellectual property lost?

- £

d. If unable to provide figure, was it:

- Less than £5,000
- £5,000 to £10,000
- £10,001 to £50,000
- £50,001 to £100,000
- £100,001 to £500,000
- £500,001 to £1 million
- More than £1 million, up to £10 million
- More than £10 million

e. How did you arrive at the estimated cost of the intellectual property loss?

- Prior internal assessment
- Prior assessment by external consultants

- Rough estimation
- Gut feeling
- Other (please state)
-

2.7 Lost commercially sensitive information other than intellectual property

a. Has the loss of commercially sensitive information resulted in the firm losing competitive advantage?

- Yes
- No

b. If yes, how did your firm determine the loss of competitive advantage?

- Emergence of new competition
- Appearance of copied products or activities
- Soured deals or business ventures
- Compromised negotiations
- Other (please state)
-

c. What was the value of the commercially sensitive information?

- £

d. If unable to provide figure, was it:

- Less than £5,000
- £5,000 to £10,000
- £10,001 to £50,000
- £50,001 to £100,000
- £100,001 to £500,000
- £500,001 to £1 million
- More than £1 million, up to £10 million
- More than £10m

e. How did you arrive at the estimated cost of the commercially sensitive information loss?

- Prior internal assessment
- Prior assessment by external consultants
- Rough estimation
- Gut feeling
- Other (please state)
-

2.8 IT equipment was damaged

a. What was the response to the IT equipment damage?

- Repairing the damaged equipment
- Replacing the damaged equipment
- Other (please state)
- [ ]

b. What was the cost of repairing/replacing the IT equipment?

- £ [ ]

c. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- £10,001 to £50,000
- £50,001 to £100,000
- £100,001 to £500,000
- £500,001 to £1 million
- More than £1 million

d. Did the damage also result in disruption or interruption of services?

- Yes
- No

e. If yes, which service was unavailable? Select all that apply.

- Email
- External client facing systems (e.g. marketing, purchasing)
- Internal systems (e.g. HR)
- Website
- Other (please state)
- [ ]

f. For each service selected above, what was the duration of time for which the service was unavailable?

- [ ] hours/days (select as appropriate)

g. For each service selected above, if unable to provide percentage, was it:

- Less than an hour
- Between an hour and a day
- 1-3 days
- 4-5 days
- 6-10 days
- More than 10 days

h. For each service selected above, is the service directly related to revenue generation?

- Yes
- No

i. If yes, for each service selected above, through which mechanism was revenue affected? Please give a brief description.

-

j. For each service selected above, what is the amount of revenue associated with the service per hour/day/month (select as appropriate)?

- £

k. For each service selected above, if unable to provide a figure, was the estimated revenue loss per day as a result of the interruption to the service:

- Less than £100
- Between £100 and £200
- £201 to £500
- £501 to £1,000
- More than £1,000

l. Was staff time required in repairing/replacing (select as appropriate) the damaged IT equipment?

- Yes
- No

m. How many staff were involved in repairing/replacing (select as appropriate) the damaged IT equipment?

-

n. How long was each staff member involved in repairing/replacing (select as appropriate) the damaged IT equipment? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

o. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in repairing/replacing (select as appropriate) the damaged IT equipment? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

p. Were external contractors required to fix the damaged IT equipment?

- Yes
- No

q. If yes, what was the amount paid to external contractors?

- £

2.9 Other physical equipment damage (not including IT equipment)

a. What was the response to the physical equipment damage?

- Repairing the damaged equipment
- Replacing the damaged equipment
- Other (please state)
-

b. What was the cost of repairing/replacing the physical equipment?

- £

c. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- £10,001 to £50,000
- £50,001 to £100,000
- £100,001 to £500,000
- £500,001 to £1 million
- More than £1 million

d. Did the damage also result in disruption or interruption of services?

- Yes
- No

e. If yes, which service was unavailable? Select all that apply.

- Email
- External client facing systems (e.g. marketing, purchasing)
- Internal systems (e.g. HR)
- Website
- Other (please state)
- [ ]

f. For each service selected above, what was the duration of time for which the service was unavailable?

- [ ] hours/days (select as appropriate)

g. If unable to provide percentage, was it:

- Less than an hour
- Between an hour and a day
- 1-3 days
- 4-5 days
- 6-10 days
- More than 10 days

h. Is the service directly related to revenue generation?

- Yes
- No

i. If yes, through which mechanism was revenue affected? Please give a brief description.

–

j. What is the amount of revenue associated with the service per hour/day/month (select as appropriate)?

– £

k. If unable to provide a figure, was the estimated revenue loss per day as a result of the interruption to the service:

- Less than £100
- Between £100 and £200
- £201 to £500
- £501 to £1,000
- More than £1,000

l. Was staff time required in repairing/replacing (select as appropriate) the damaged physical equipment?

- Yes
- No

m. If yes, how many staff were involved in repairing/replacing (select as appropriate) the damaged physical equipment?

–

n. For how long was each staff member involved in repairing/replacing (select as appropriate) the damaged physical equipment? Insert more columns as required.

Staff member 1 hours/days	**Staff member 2 hours/days**	**Staff member 3 hours/days**

o. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in repairing/replacing (select as appropriate) the damaged physical equipment? Insert more columns as required.

Staff member/band 1	**Staff member/band 2**	**Staff member/band 3**
£	£	£

p. Were external contractors required to fix the damaged physical equipment?

- Yes
- No

q. If yes, what was the amount paid to external contractors?

- £

2.10 Paid an insurance excess

a. What was the value of the payment made?

- £

b. If unable to provide a figure, was it:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

3 Legal or regulatory costs

For these questions, you may need to talk to **someone in a legal or compliance role**, such as a Data Protection Officer, or anyone else that deals with industry regulators.

3.1 Fines by regulators or authorities

a. What was the sum of the fines by regulators or authorities?

– £

b. If unable to provide a figure, was it:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

3.2 Legal action by those impacted by the breach

a. Was your organisation forced to seek external legal advice as a result of the legal action taken as a result of the breach?

- Yes
- No

b. If yes, what was the cost of engaging legal advice?

– £

c. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

d. Were internal staff were involved in the legal proceedings?

- Yes
- No

e. If yes, how many internal staff were involved?

–

f. For how long was each staff member involved in legal proceedings? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

g. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in legal proceedings? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

h. Were any payments made as a result of legal action?

- Yes
- No

i. If yes, what was the sum of these payments?

- £

j. If unable to provide a figure, was it:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

3.3 You had to notify the authorities (e.g. police or a regulator)

a. Was staff time involved in the notification of the authorities?

- Yes
- No

b. If yes, how many internal staff were involved?

-

c. For how long was each staff member involved in the notification of the authorities? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

d. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in the notification of the authorities? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

e. What other costs were involved in notifying the authorities? Insert more columns as required.

Telephone costs	Mailing costs	Other costs
£	£	£

3.4 You had to notify customers, investors, suppliers or any other people or organisations you work with

a. Was staff time involved in the notification of customers or other stakeholders?

- Yes
- No

b. If yes, how many internal staff were involved?

-

c. For how long was each staff member involved in the notification of customers or other stakeholders? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

d. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in the notification of customers or other stakeholders? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

e. What other costs were involved in notifying customers or other stakeholders? Insert more columns as required.

Telephone costs	Mailing costs	Other costs
£	£	£

4 Costs related to technical cyber security teams or practices

4.1 You chose to shut down at-risk services (e.g. software applications or networks) to prevent further exposure to the breach

a. Which activities were shut down?

- External/client facing systems e.g. marketing, purchasing)
- Website
- Email
- Internal systems e.g. HR
- Other (please state)
- _____

b. Did this result in disruption or interruption of business as usual activities?

- Yes
- No

c. If yes, which service was unavailable? Select all that apply.

- Email
- External client facing systems (e.g. marketing, purchasing)
- Internal systems (e.g. HR)
- Website
- Other (please state)
- _____

d. For each service selected above, was the service partially or completely unavailable?

- Completely unavailable
- Partially unavailable

e. For each service selected above, if partially unavailable, to what extent was the service unavailable (where 100% is completely unavailable)?

- _____ %

f. For each service selected above, if unable to provide percentage, was it:

- Less than 20% unavailable
- 20%-40% unavailable
- 41%-60% unavailable
- 61%-80% unavailable
- More than 80% unavailable

g. For each service selected above, what was the duration of time for which the service was unavailable?

– [ ] hours/days (select as appropriate)

h. For each service selected above, if unable to provide percentage, was it:

- Less than an hour
- Between an hour and a day
- 1-3 days
- 4-5 days
- 6-10 days
- More than 10 days

i. For each service selected above, is the service directly related to revenue generation?

- Yes
- No

j. If yes, for each service selected above, through which mechanism was revenue affected? Please give a brief description.

–

k. For each service selected above, what is the amount of revenue associated with the service per hour/day/month (select as appropriate)?

– £

l. For each service selected above, if unable to provide a figure, was the estimated revenue loss per day as a result of the interruption to the service:

- Less than £100
- Between £100 and £200
- £201 to £500
- £501 to £1,000
- More than £1,000

m. Was staff time required to shut down the at-risk services?

- Yes
- No

n. If yes, how many internal staff were involved?

–

o. For how long was each staff member required to shut down the at-risk services? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

p. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those required to shut down the at-risk services? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

q. Were external consultants hired to shut down high risk services?

- Yes
- No

r. What was the cost of contracting these external services?

- £

s. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

4.2 Existing staff had to work overtime to resolve the breach

a. What was the total cost of the overtime required to resolve the breach?

- £

b. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

4.3 You had to hire additional staff or engage an external cyber security provider or consultant on a temporary basis to help resolve the breach

a. Did these staff work exclusively on the breach?

- Yes
- No

b. If no, what proportion of time was spent resolving the breach (where 100% is all their time)?

- _____ %

c. What was the total cost of hiring short-term workers?

- £_____

d. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

4.4 You spent time investigating the source of the breach

a. Was staff time required to investigate the source of the breach?

- Yes
- No

b. If yes, how many internal staff were involved?

- _____

c. For how long was each staff member required to investigate the source of the breach? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

d. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those required to investigate the source of the breach? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

e. Where external contractors involved in investigating the breach?

- Yes
- No

f. If yes, what was the cost of contracting external workers to investigate the breach?

- £

g. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

4.5 Provided additional cyber security protection to customers, investors, suppliers or any other people or organisations you work with

a. What additional cyber protection was provided? Please give a brief description.

-

b. Not including staff time, what was the cost of each additional security measure? Provide figure for each of the additional cyber protection features provided. Insert more columns as required.

Measure 1	Measure 2	Measure 3
£	£	£

c. Was staff time involved in providing additional cyber protection to customers or other stakeholders?

- Yes
- No

d. If yes, how many internal staff were involved?

-

e. For how long was each staff member involved in providing additional cyber protection to customers or other stakeholders? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

f. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in providing additional cyber protection to customers or other stakeholders? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

g. Were external consultants contracted to provide additional cyber protection to customers/ stakeholders?

- Yes
- No

h. What was the cost of contracting external workers to change the cyber security practices?

- £

i. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

4.6 Changed any internal IT or cyber security policies, technical controls, processes or providers (e.g. internet service providers or software providers)

a. Which cyber security practices were changed? Please give a brief description.

-

b. Was staff time involved in these changes to cyber security practices?

- Yes
- No

c. If yes, how many internal staff were involved?

–

d. For how long was each staff member involved in these changes to cyber security practices? Insert more columns as required.

Staff member 1 hours/days	**Staff member 2 hours/days**	**Staff member 3 hours/days**

e. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in these changes to cyber security practices? Insert more columns as required.

Staff member/band 1	**Staff member/band 2**	**Staff member/band 3**
£	£	£

f. Were external consultants involved in changing cyber security practices?

- Yes
- No

g. If yes, what was the cost of contracting external workers to change the cyber security practices?

– £

h. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

i. What other costs, if any, were involved in changing the organisation's cyber security practices? Provide figure for each of the additional costs. Insert more columns as required.

Measure 1	**Measure 2**	**Measure 3**
£	£	£

4.7 Hired new staff, permanently increased hours of existing staff or engaged external cyber security providers on a permanent basis, or carried out more staff training on cyber security

a. What long term changes in cyber security practices were made?

- Hiring new cyber security staff
- Increase in cyber security training
- Other (please state)
- _____

b. If you selected hired new cyber security staff, how many new cyber security staff were hired?

- _____

c. Were these staff hired as a direct result of the breach or only partially as a result?

- Direct result of the breach
- Partially as a result of the breach, but also as result of other factors

d. If partially, to what extent was the breach a factor in the hiring of these new staff (where 100% means they were hired directly as a result of the breach)?

- _____ %

e. If unable to provide percentage, was it:

- Less than 20%
- 20%-40%
- 41%-60%
- 61-80%
- More than 80%

f. What is the yearly wage of each of these new cyber security staff? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

g. If you selected increase in cyber security training, was the training internal or external?

- Internal
- External

h. If external, what was the cost of the external training?

- £_____

i. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

j. If internal, how many staff were involved in conducting the training?

–

k. How much staff time was involved in preparing and conducting the training? Insert more columns as required.

Staff member 1 hours/days	**Staff member 2 hours/days**	**Staff member 3 hours/days**

l. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in preparing and conducting the training? Insert more columns as required.

Staff member/band 1	**Staff member/band 2**	**Staff member/band 3**
£	£	£

m. How many staff attended the training?

–

n. How many hours did the training session last?

–

o. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those attending the training? Insert more columns as required.

Staff member/band 1	**Staff member/band 2**	**Staff member/band 3**
£	£	£

p. What were the additional costs involved in the training, if any? Please give a brief description.

–

q. What was the cost of each item you describe (e.g. rooms, materials or other equipment)? Provide figure for each of the additional costs. Insert more columns as required.

Cost 1	**Cost 2**	**Cost 3**
£	£	£

5 Other costs to the whole organisation

5.1 You provided compensation (e.g. money or vouchers) to the customers, investors, suppliers or any other people or organisations you work with

a. What was the overall amount of compensation provided to impacted customers or other stakeholders of the breach?

– £

b. If unable to provide a figure, were they:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

5.2 You provided discounts to customers

a. What was the total sum of discounts provided to impacted customer or other stakeholders impacted by the breach?

– £

b. If unable to provide a figure, were they:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

5.3 You had to deal with complaints (e.g. from those impacted by the breach)

a. Was staff time required to deal with complaints?

- Yes
- No

b. If yes, how many internal staff were involved?

–

c. For how long was each staff member required to deal with complaints? Insert more columns as required.

Staff member 1 hours/days	**Staff member 2 hours/days**	**Staff member 3 hours/days**

d. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those required to deal with complaints? Insert more columns as required.

Staff member/band 1	**Staff member/band 2**	**Staff member/band 3**
£	£	£

e. Were external consultants hired to shut down at-risk services?

- Yes
- No

f. If yes, what was the cost of contracting these external services?

- £

g. If unable to provide a figure, were they:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

h. What other resources, if any, were involved in dealing with complaints from those impacted by the breach? Please give a brief description.

-

i. What was the cost of each item you describe (e.g. hiring out a call centre)? Provide figure for each of the additional costs. Insert more columns as required.

Cost 1	**Cost 2**	**Cost 3**
£	£	£

5.4 Engaged in PR or marketing activities in response to the breach (e.g. on social media, advertising or any other communications)

a. Were these PR or marketing activities a direct result of the breach or partially as a result of the breach (i.e. you were going to do them anyway)?

- Exclusively a result of the breach
- Partially a result of the breach

b. If partially, how much would you say these PR or marketing activities would you say were in response to the breach (where 100% is all these PR or marketing activities)?

- [ ] %

c. If unable to provide a percentage, was it:

- Less than 20% of the reason
- 21%-40% of the reason
- 41%-60% of the reason
- 61%-80% of the reason
- More than 80% of the reason

d. Were external consultants contracted to conduct PR or marketing activities?

- Yes
- No

e. If yes, what was the fee paid to contract these external services?

- [ ] £

f. If unable to provide a figure, were they:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

g. Was staff time involved in PR or marketing activities?

- Yes
- No

h. If yes, how many internal staff were involved?

- [ ]

i. For how long was each staff member involved in PR or marketing activities? Insert more columns as required.

Staff member 1 hours/days	Staff member 2 hours/days	Staff member 3 hours/days

j. What was the hourly/daily/weekly/monthly/yearly (select as appropriate) wage of those involved in PR or marketing activities? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

k. What other resources were involved in conducting PR or marketing activities? Please give a brief description.

–

l. What was the cost of each item you describe (e.g. buying advertising space offline or online)? Provide figure for each of the additional costs. Insert more columns as required.

Cost 1	Cost 2	Cost 3
£	£	£

5.5 A reduction in investment or donor funding

a. Was breach completely or partially responsible for the reduction in investment or donor funding?

- Completely responsible
- Partially responsible

b. If partially, to what extent would you say the breach was responsible for the reduction in investment or donor funding (where 100% is completely responsible)?

– %

c. If unable to provide a figure, was it:

- Less than 20% responsible
- 21%-40% responsible
- 41%-60% responsible
- 61%-80% responsible
- More than 80% responsible

d. By how much did investment/donor funding fall?

– £

e. If unable to provide a figure, was it:

- Less than £1,000
- £1,000 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- £10,000 to £50,000
- £50,001 to £100,000
- More than £100,000

5.6 You decided to reduce spending on research and development or investing in a new production process or technology as a direct result of the breach

a. By how much was investment in research and development or investment in a new production process or technology reduced as a result of the breach?

– £

b. If unable to provide a figure, was it:

- Less than £1,000
- £1,000 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- £10,000 to £50,000
- £50,001 to £100,000
- More than £100,000

5.7 Downgrading of credit rating

a. By how much did the credit rating decline?

Pre-breach credit rating	Post-breach credit rating

b. By how much did this change in the credit rating lead to any increase the amount the firm payed to service its loans?

– £

c. If unable to provide a figure, was it:

- Less than £250
- £250 to £500
- £501 to £1,000

- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- More than £10,000

5.8 Increase in any insurance premiums

a. By how much did insurance premiums increase?

- £

b. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

5.9 Increased difficulty in recruiting new staff

a. Was the breach completely responsible for the increased difficulties in recruiting new staff?

- Yes, completely responsible
- No, only partially responsible

b. If only partially responsible, to what extent was the breach responsible for increased hiring costs?

- Less than 20%
- 20%-40% responsible
- 41%-60% responsible
- 61-80% responsible
- More than 80% responsible

c. How many new recruits have been made following the breach?

-

d. For each new hire, how much have recruitment costs increased? Insert more columns as required.

Staff member/band 1	Staff member/band 2	Staff member/band 3
£	£	£

e. For each new hire, if unable to provide a figure, was it:

- Less than £250
- £250 to £500
- £501 to £1,000
- £1,001 to £2,500
- £2,501 to £5,000
- £5,001 to £10,000
- More than £10,000

5.10 You lost customers

a. How many customers have been lost as a **direct result** of the breach?

- £

b. If unable to provide a figure was it:

- Less than £100
- £101 to £500
- £501 to £1,000
- £1,001 to £5,000
- £5,001 to £10,000
- More than £10,000

c. What is the average revenue lost associated with each customer?

- £

d. If unable to provide a figure, was it:

- Less than £10
- £10 to £50
- £51 to £100
- £101 to £200
- £201 to £500
- £501 to £1,000
- £1,000 to £2,000
- More than £2,000

5.11 You lost suppliers

a. How many suppliers were lost as a result of the breach?

-

b. For each supplier lost, is the breach completely or partially responsible for this?

- Breach completely responsible
- Breach partially responsible

c. For each supplier lost, if partially responsible, to what extent was the breach responsible (where 100% is completely responsible)?

- _____ %

d. For each supplier lost, if unable to provide figure, was it:

- Less than 20%
- 20%-40%
- 41%-60%
- 61-80%
- More than 80%

e. For each supplier lost, what action has been taken in response to the loss?

- Switching to another supplier
- Other (please state)
- _____

f. For each supplier lost, what has been the estimated cost of losing this supplier?

Supplier 1	**Supplier 2**	**Supplier 3**
£	£	£

g. If unable to provide figure, was it:

- Less than £500
- £500 to £1,000
- £1,001 to £2,000
- £2,001 to £5,000
- £5,001 to £10,000
- £10,001 to £50,000
- £50,001 to £100,000
- More than £100,000

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

Ipsos MORI