



Data Protection Survey

Data Report

- 1 How many employees work in your organisation?
- 2 Within which sector is your organisation?
- 3 What does your business spend annually on IT security?
- 4 Have you invested in DLP solutions?
- 5 What approximate percentage of your overall IT security budget is spent on DLP solutions?
- 6 Which of the statements below best describes your current plans for future investment in DLP solutions?
- 7 You have said that you do not currently, or will not be investing in DLP. What do you regard as the main barriers to adoption of DLP in your organisation?
- 8 Has your organisation conducted an assessment of the business risks associated with data leakage?
- 9 Which of the following priorities are the strongest drivers of your organisation's data security strategy?
- 10 Does your organisation have a security policy and documented procedures for protecting data?
- 11 Does your organisation have a policy and procedure framework that addresses the actions that need to be taken after a security incident involving data leakage has occurred?
- 12 Who is responsible for DLP within your organisation?
- 13 You said that a single person is responsible for DLP within your organisation. Who is responsible for DLP within your organisation?
- 14 You said that several people are responsible for DLP within your organisation. Which of the following are responsible for DLP within your organisation?
- 15 Does your organisation support remote/mobile working?
- 16 How has your organisation's use of remote/mobile working changed over the past 1 - 2 years?
- 17 How has this increase in remote working affected your data security strategy?
- 18 Which of the DLP measures below are you employing to manage the risk this raises?
- 19 Does your organisation allow the use of employee-owned devices at work, such as iPads, tablets, laptops, and/or smartphones?
- 20 Which of the DLP measures below are you employing to manage the risk this raises?
- 21 Does your organisation classify and monitor its data (e.g. where it is, how it moves, who has access to it, etc.)?
- 22 To what extent do you agree with the following statement? "We are currently not conducting data classification and monitoring for data security purposes because seeing evidence of leaks will require investments and a focus in DLP that our organisation is unable or not ready to make."
- 23 How likely do you think it is that your organisation will experience a data leakage incident involving sensitive, valuable or confidential data in the foreseeable future?
- 24 What was the type of data leakage incident your company has experienced?
- 25 Did the incident damage your organisation in any way?
- 26 Which of the following best fits the way in which the incident damaged your organisation?
- 27 If possible, please quantify how much the incident damaged your organisation:
- 28 How likely do you think it would be for an incident to damage your organisation in some way?
- 29 Which of the technologies below do you regard as representing the greatest data leakage risk to your organisation?
- 30 What type of data leakage threat are you most concerned about?
- 31 What are you most worried about in terms of damage from a data leak incident?
- 32 To what extent do you agree with the following statement? "Opening up corporate data to employees to support mobility and productivity significantly increases the risk of serious/damaging data leakage incidents."
- 33 To what extent do you agree with the following statement? "The use of employee-owned devices at work significantly increases the risk of serious/damaging data leakage incidents."
- 34 To what extent do you agree with the following statement? "The WikiLeaks data leak and associated events has made me take a closer look at DLP solutions."
- 35 Do you think your organisation has experienced a leakage of sensitive/confidential/valuable information that you are not aware of?
- 36 Do you think it may have damaged your organisation?
- 37 In what way might your organisation have been damaged?

How many employees work in your organisation?

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
500 - 1000	22%	20%	21%	20%	21%
1000 - 3000	27%	25%	36%	20%	46%
More than 3000	51%	55%	42%	60%	33%
Base	200	44	33	30	24

Within which sector is your organisation?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Financial services	22%	20%	20%	24%
Technology	15%	14%	9%	19%
Government and education	13%	16%	13%	11%
FMCG, retail, wholesale	10%	11%	9%	10%
Professional services	10%	11%	19%	5%
Energy and utilities	7%	11%	4%	7%
Transport and logistics	5%	2%	2%	8%
Healthcare	4%	0%	7%	3%
Construction	3%	7%	0%	2%
Automotive	2%	0%	4%	2%
Media and entertainment	2%	2%	4%	0%
Service providers	2%	0%	0%	3%
Pharmaceuticals	1%	2%	0%	1%
Non-profit	1%	0%	2%	0%
Real estate and hospitality	1%	0%	2%	0%
*Other, please specify	6%	2%	6%	7%
Base	200	44	54	102

*Other, please specify: "Electrical manufacturing", "Infrastructure", "Manufacturing" x7, "Manufacturing : Packaging", "Oil/Gas".

What does your business spend annually on IT security?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
£0-£49,999	8%	23%	7%	2%
£50,000-£99,999	10%	11%	20%	4%
£100,000-£249,999	15%	18%	17%	12%
£250,000-£499,999	9%	2%	7%	13%
£500,000-£999,999	12%	14%	19%	7%
£1 million - £2 million	24%	25%	13%	29%
More than £2 million	14%	5%	7%	22%
Don't know	9%	2%	9%	12%
Average	£1,027,335	£683,720	£693,877	£1,373,055
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
£0-£49,999	8%	2%	18%	17%	4%
£50,000-£99,999	10%	0%	6%	23%	13%
£100,000-£249,999	15%	9%	21%	13%	29%
£250,000-£499,999	9%	9%	0%	7%	17%
£500,000-£999,999	12%	11%	18%	3%	4%
£1 million - £2 million	24%	36%	12%	23%	13%
More than £2 million	14%	25%	6%	10%	13%
Don't know	9%	7%	18%	3%	8%
Average	£1,027,335	£1,535,975	£667,592	£770,689	£782,954
Base	200	44	33	30	24

Have you invested in DLP solutions?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	59%	61%	50%	62%
No	42%	39%	50%	38%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	59%	64%	58%	27%	63%
No	42%	36%	42%	73%	38%
Base	200	44	33	30	24

What approximate percentage of your overall IT security budget is spent on DLP solutions?

Base: Only asked of respondents have invested in DLP solutions

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Less than 5%	12%	0%	15%	16%
Between 5 and 10%	19%	11%	30%	17%
Between 10 and 15%	20%	22%	15%	21%
Between 15 and 20%	21%	48%	19%	11%
Between 20 and 25%	15%	11%	15%	16%
Between 25% and 30%	5%	4%	4%	6%
More than 30%, please specify	0%	0%	0%	0%
Don't know	9%	4%	4%	13%
Average	13.76%	16.15%	12.50%	13.23%
Base	117	27	27	63

Base: Only asked of respondents have invested in DLP solutions

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Less than 5%	12%	7%	21%	13%	0%
Between 5 and 10%	19%	11%	32%	13%	27%
Between 10 and 15%	20%	25%	5%	13%	13%
Between 15 and 20%	21%	29%	11%	0%	33%
Between 20 and 25%	15%	21%	11%	38%	20%
Between 25% and 30%	5%	0%	0%	25%	0%
More than 30%, please specify	0%	0%	0%	0%	0%
Don't know	9%	7%	21%	0%	7%
Average	13.76%	15.00%	9.83%	18.13%	15.00%
Base	117	28	19	8	15

Which of the statements below best describes your current plans for future investment in DLP solutions?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Broad DLP portfolio solutions (such as DLP suites from McAfee, RSA, Websense or Symantec)	30%	39%	30%	26%
Point solutions that solve key challenges (such as endpoint encryption, web content security, etc.)	25%	32%	24%	23%
Assessments to identify our risks around data leakage	16%	7%	15%	21%
Integration services to link existing security technology to a data security strategy (i.e. making the most of existing solutions in place)	13%	11%	7%	17%
We don't have any investment plans for DLP	11%	11%	19%	7%
Don't know	5%	0%	6%	7%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Broad DLP portfolio solutions (such as DLP suites from McAfee, RSA, Websense or Symantec)	30%	34%	21%	7%	42%
Point solutions that solve key challenges (such as endpoint encryption, web content security, etc.)	25%	27%	39%	23%	21%
Assessments to identify our risks around data leakage	16%	11%	18%	20%	13%
Integration services to link existing security technology to a data security strategy (i.e. making the most of existing solutions in place)	13%	14%	3%	17%	8%
We don't have any investment plans for DLP	11%	7%	9%	27%	13%
Don't know	5%	7%	9%	7%	4%
Base	200	44	33	30	24

You have said that you do not currently, or will not be investing in DLP. What do you regard as the main barriers to adoption of DLP in your organisation?

Base: Only asked of respondents who have not invested, or will not be investing in DLP solutions

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Other IT spending priorities take precedence	57%	59%	48%	63%
Lack of board level interest/will to invest	30%	59%	41%	10%
We don't know if we need it or not	29%	41%	41%	15%
It requires data classification and monitoring	20%	29%	11%	23%
We don't know what it encompasses	19%	12%	26%	18%
It's too complex to deploy	18%	24%	15%	18%
We don't believe it will work – i.e. actually stop data leaking	14%	12%	4%	23%
The risk of data leakage is not great enough to bother with it	14%	12%	11%	18%
It's too costly	14%	18%	11%	15%
Damage from a data leakage incident is too unlikely to warrant investment	13%	18%	19%	8%
We don't know who should be responsible for leading or managing it	11%	12%	15%	8%
We don't need it	4%	0%	0%	8%
*Other, please specify	5%	0%	11%	3%
Base	84	17	27	40

*Other, please specify: "Outsourced this responsibility", "No expertise within the organisation", "We operate online game services, a corporate office network, hence DLP risks are more specific".

Base: Only asked of respondents who have not invested, or will not be investing in DLP solutions

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Other IT spending priorities take precedence	57%	31%	67%	68%	56%
Lack of board level interest/will to invest	30%	13%	47%	36%	22%
We don't know if we need it or not	29%	19%	40%	27%	44%
It requires data classification and monitoring	20%	13%	40%	5%	22%
We don't know what it encompasses	19%	13%	40%	23%	11%
It's too complex to deploy	18%	25%	7%	9%	22%
We don't believe it will work – i.e. actually stop data leaking	14%	13%	13%	5%	11%
The risk of data leakage is not great enough to bother with it	14%	13%	13%	23%	11%
It's too costly	14%	19%	20%	14%	0%
Damage from a data leakage incident is too unlikely to warrant investment	13%	6%	13%	32%	0%
We don't know who should be responsible for leading or managing it	11%	6%	27%	9%	11%
We don't need it	4%	19%	0%	0%	0%
Other, please specify	5%	6%	0%	5%	0%
Base	84	16	15	22	9

Has your organisation conducted an assessment of the business risks associated with data leakage?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	69%	73%	57%	74%
No	31%	27%	43%	26%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	69%	84%	61%	60%	63%
No	31%	16%	39%	40%	38%
Base	200	44	33	30	24

Which of the following priorities are the strongest drivers of your organisation's data security strategy?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Compliance	58%	50%	52%	65%
Cost saving	40%	45%	30%	43%
Improving efficiency	40%	57%	35%	34%
Mobility	35%	36%	28%	37%
Virtualisation	33%	39%	31%	30%
Improving productivity	33%	50%	28%	27%
Cloud computing	30%	34%	26%	30%
Customer acquisition and retention	25%	18%	22%	28%
Organisation growth	23%	27%	20%	22%
Supporting innovation and R&D	19%	34%	11%	17%
The question is irrelevant as we don't have a data security strategy	3%	5%	6%	0%
*Other, please specify	2%	0%	4%	1%
Base	200	44	54	102

*Other, please specify: "Confidentiality", "Minimise financial risk", "Publicity".

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Compliance	58%	59%	76%	63%	58%
Cost saving	40%	34%	42%	40%	38%
Improving efficiency	40%	41%	45%	53%	25%
Mobility	35%	45%	30%	17%	42%
Virtualisation	33%	30%	27%	23%	46%
Improving productivity	33%	32%	27%	33%	29%
Cloud computing	30%	27%	15%	20%	46%
Customer acquisition and retention	25%	23%	12%	37%	17%
Organisation growth	23%	30%	15%	30%	13%
Supporting innovation and R&D	19%	20%	6%	7%	4%
The question is irrelevant as we don't have a data security strategy	3%	2%	3%	7%	4%
Other, please specify	2%	0%	3%	3%	0%
Base	200	44	33	30	24

Does your organisation have a security policy and documented procedures for protecting data?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	94%	95%	91%	95%
No	6%	5%	9%	5%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	94%	89%	94%	87%	100%
No	6%	11%	6%	13%	0%
Base	200	44	33	30	24

Does your organisation have a policy and procedure framework that addresses the actions that need to be taken after a security incident involving data leakage has occurred?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	81%	75%	74%	87%
No	19%	25%	26%	13%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	81%	89%	79%	77%	83%
No	19%	11%	21%	23%	17%
Base	200	44	33	30	24

Who is responsible for DLP within your organisation?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
A number of people	60%	59%	50%	66%
A single person	27%	30%	30%	24%
No one in particular	7%	11%	7%	5%
No one at all	2%	0%	6%	1%
Don't know	5%	0%	7%	5%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
A number of people	60%	57%	55%	53%	58%
A single person	27%	30%	27%	30%	17%
No one in particular	7%	5%	3%	10%	21%
No one at all	2%	5%	0%	3%	0%
Don't know	5%	5%	15%	3%	4%
Base	200	44	33	30	24

You said that a single person is responsible for DLP within your organisation. Who is responsible for DLP within your organisation?

Base: Only asked of respondents whose company have invested in DLP solutions and said a single person is responsible for DLP within their organisation.

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Security manager	25%	0%	19%	42%
IT director	19%	31%	19%	13%
CIO	15%	38%	6%	8%
IT manager	15%	31%	0%	17%
Security director	8%	0%	19%	4%
Compliance manager	6%	0%	6%	8%
CEO	4%	0%	6%	4%
CSO	4%	0%	13%	0%
MD	2%	0%	0%	4%
Risk manager	2%	0%	6%	0%
Network manager	0%	0%	0%	0%
Data centre manager	0%	0%	0%	0%
CFO	0%	0%	0%	0%
*Other, please specify	2%	0%	6%	0%
Don't know	0%	0%	0%	0%
Base	53	13	16	24

*Other, please specify: "Information security officer".

Base: Only asked of respondents whose company have invested in DLP solutions and said a single person is responsible for DLP within their organisation.

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Security manager	25%	23%	44%	11%	0%
IT director	19%	15%	33%	11%	25%
CIO	15%	23%	0%	22%	0%
IT manager	15%	8%	22%	11%	0%
Security director	8%	15%	0%	0%	25%
Compliance manager	6%	0%	0%	22%	0%
CEO	4%	0%	0%	11%	25%
CSO	4%	8%	0%	0%	25%
MD	2%	8%	0%	0%	0%
Risk manager	2%	0%	0%	11%	0%
Network manager	0%	0%	0%	0%	0%
Data centre manager	0%	0%	0%	0%	0%
CFO	0%	0%	0%	0%	0%
Other, please specify	2%	0%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%
Base	53	13	9	9	4

You said that several people are responsible for DLP within your organisation. Which of the following are responsible for DLP within your organisation?

Base: Only asked of respondents whose company have invested in DLP solutions and said a several people are responsible for DLP within their organisation.

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
IT director	53%	50%	63%	49%
Security manager	42%	35%	37%	46%
IT manager	36%	54%	37%	28%
Security director	35%	27%	22%	43%
Compliance manager	29%	15%	26%	36%
CIO	28%	31%	19%	30%
Risk manager	23%	15%	19%	28%
Network manager	23%	15%	30%	22%
CEO	18%	15%	11%	22%
Data centre manager	13%	19%	11%	12%
CSO	8%	4%	4%	12%
CFO	8%	0%	7%	10%
MD	5%	4%	4%	6%
*Other, please specify	3%	0%	11%	0%
Don't know	1%	0%	0%	1%
Base	120	26	27	67

*Other, please specify: "Commercial manager", "Information Governance", "Service delivery".

Base: Only asked of respondents whose company have invested in DLP solutions and said a several people are responsible for DLP within their organisation.

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
IT director	53%	56%	39%	56%	64%
Security manager	42%	32%	39%	38%	43%
IT manager	36%	28%	22%	56%	36%
Security director	35%	48%	17%	31%	21%
Compliance manager	29%	36%	11%	38%	29%
CIO	28%	40%	28%	13%	7%
Risk manager	23%	20%	17%	13%	43%
Network manager	23%	16%	17%	25%	29%
CEO	18%	24%	28%	6%	0%
Data centre manager	13%	24%	0%	25%	21%
CSO	8%	8%	11%	13%	7%
CFO	8%	8%	0%	19%	0%
MD	5%	0%	0%	0%	7%
Other, please specify	3%	0%	6%	6%	0%
Don't know	1%	0%	0%	0%	0%
Base	120	25	18	16	14

Does your organisation support remote/mobile working?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	96%	95%	94%	96%
No	5%	5%	6%	4%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	96%	89%	100%	93%	96%
No	5%	11%	0%	7%	4%
Base	200	44	33	30	24

How has your organisation's use of remote/mobile working changed over the past 1 - 2 years?

Base: Only asked of respondents whose organisations support remote working

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Increased	81%	83%	82%	80%
Decreased	4%	2%	6%	3%
Stayed constant	15%	14%	10%	17%
Don't know	1%	0%	2%	0%
Base	191	42	51	98

Base: Only asked of respondents whose organisations support remote working

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Increased	81%	82%	88%	68%	78%
Decreased	4%	3%	0%	7%	9%
Stayed constant	15%	15%	9%	25%	13%
Don't know	1%	0%	3%	0%	0%
Base	191	39	33	28	23

How has this increase in remote working affected your data security strategy?

Base: Only asked of respondents whose organisations support remote working and have seen it increase

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
It's made data security more important	84%	83%	74%	90%
It's made data security less important	0%	0%	0%	0%
It's had no effect	15%	17%	24%	10%
Don't know	1%	0%	2%	0%
Base	155	35	42	78

Base: Only asked of respondents whose organisations support remote working and have seen it increase

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
It's made data security more important	84%	75%	83%	84%	89%
It's made data security less important	0%	0%	0%	0%	0%
It's had no effect	15%	25%	17%	16%	11%
Don't know	1%	0%	0%	0%	0%
Base	155	32	29	19	18

Which of the DLP measures below are you employing to manage the risk this raises?

Base: Only asked of respondents whose organisations support remote working

	Total	500 - 1000 employees	1000 - 3000 employees	3000 employees
Anti-virus	83%	93%	76%	83%
Content blocking	68%	62%	69%	70%
Anti-SPAM	66%	62%	63%	69%
SMTP encryption	54%	57%	43%	58%
Content control	53%	60%	37%	59%
Protocol inspection	31%	29%	29%	33%
Process control	30%	33%	22%	33%
Application inspection	27%	29%	24%	29%
*Other, please specify	4%	7%	6%	2%
None of these	1%	0%	2%	0%
Don't know	2%	0%	4%	2%
Base	191	42	51	98

*Other, please specify: "Air-gap separated networks", "Encryption of all data assets outside of offices", "Enforcing PIN codes on mobile devices", "Hard drive encryption", "Laptop encryption", "Specific function access regarding apps and data", "VPN" x2.

Base: Only asked of respondents whose organisations support remote working

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Anti-virus	83%	77%	79%	93%	87%
Content blocking	68%	54%	64%	82%	74%
Anti-SPAM	66%	56%	70%	71%	65%
SMTP encryption	54%	67%	45%	29%	57%
Content control	53%	62%	55%	57%	30%
Protocol inspection	31%	46%	33%	21%	22%
Process control	30%	51%	24%	14%	13%
Application inspection	27%	44%	9%	18%	17%
Other, please specify	4%	5%	9%	4%	0%
None of these	1%	3%	0%	0%	0%
Don't know	2%	0%	9%	0%	0%
Base	191	39	33	28	23

Does your organisation allow the use of employee-owned devices at work, such as iPads, tablets, laptops, and/or smartphones?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	51%	64%	44%	49%
No	49%	36%	56%	51%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	51%	55%	42%	47%	58%
No	49%	45%	58%	53%	42%
Base	200	44	33	30	24

Which of the DLP measures below are you employing to manage the risk this raises?

Base: Only asked of respondents whose organisation allows employee owned devices in the workplace

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Encryption	61%	54%	58%	66%
Device control	53%	54%	50%	54%
Anti-virus	49%	61%	42%	46%
Application control	39%	54%	33%	34%
Process control	37%	64%	42%	20%
Host IPDS	29%	29%	33%	28%
*Other, please specify	4%	0%	4%	6%
None of these	7%	4%	8%	8%
Base	102	28	24	50

*Other, please specify: "Firewalls for personal devices, PDA's and Smart Phones get specific email apps that are protected", "Separation of networks", "Use of consumer devices limited to R&D functions and Executives". Would not disclose x1.

Base: Only asked of respondents whose organisation allows employee owned devices in the workplace

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Encryption	61%	71%	64%	36%	50%
Device control	53%	79%	36%	50%	29%
Anti-virus	49%	63%	50%	43%	43%
Application control	39%	42%	21%	36%	29%
Process control	37%	50%	7%	29%	36%
Host IPDS	29%	42%	7%	14%	29%
Other, please specify	4%	0%	7%	0%	0%
None of these	7%	0%	14%	7%	14%
Base	102	24	14	14	14

Does your organisation classify and monitor its data (e.g. where it is, how it moves, who has access to it, etc.)?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	73%	64%	72%	77%
No	27%	36%	28%	23%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	73%	77%	70%	60%	67%
No	27%	23%	30%	40%	33%
Base	200	44	33	30	24

To what extent do you agree with the following statement? "We are currently not conducting data classification and monitoring for data security purposes because seeing evidence of leaks will require investments and a focus in DLP that our organisation is unable or not ready to make."

Base: Only asked of respondents whose organisations do not monitor or classify data

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
5 - Totally agree	13%	0%	27%	13%
4 - Somewhat agree	50%	75%	47%	35%
3 - Neither agree nor disagree	19%	13%	13%	26%
2 - Somewhat disagree	13%	13%	0%	22%
1 - Totally disagree	4%	0%	13%	0%
Don't know	2%	0%	0%	4%
Average	3.57	3.63	3.73	3.41
Base	54	16	15	23

Base: Only asked of respondents whose organisations do not monitor or classify data

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
5 - Totally agree	13%	10%	10%	25%	0%
4 - Somewhat agree	50%	30%	70%	50%	63%
3 - Neither agree nor disagree	19%	40%	0%	8%	25%
2 - Somewhat disagree	13%	10%	20%	17%	13%
1 - Totally disagree	4%	0%	0%	0%	0%
Don't know	2%	10%	0%	0%	0%
Average	3.57	3.44	3.70	3.83	3.50
Base	54	10	10	12	8

How likely do you think it is that your organisation will experience a data leakage incident involving sensitive, valuable or confidential data in the foreseeable future?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
It's already happened	10%	2%	7%	15%
It hasn't happened yet, but it's inevitable that it will	17%	14%	22%	16%
Very likely	13%	25%	13%	7%
Likely	24%	23%	22%	25%
Unlikely	24%	20%	24%	25%
Very unlikely	9%	11%	7%	8%
Will never happen	1%	0%	2%	1%
Don't know	3%	5%	2%	3%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
It's already happened	10%	9%	12%	10%	4%
It hasn't happened yet, but it's inevitable that it will	17%	7%	3%	23%	33%
Very likely	13%	20%	6%	3%	13%
Likely	24%	14%	45%	20%	17%
Unlikely	24%	32%	24%	27%	25%
Very unlikely	9%	14%	6%	7%	8%
Will never happen	1%	2%	0%	3%	0%
Don't know	3%	2%	3%	7%	0%
Base	200	44	33	30	24

What was the type of data leakage incident your company has experienced?

Base: Only asked of respondents who have experienced a data leakage incident

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Accidental data loss by employees	50%	0%	75%	47%
Internal fraud or intentional data theft by employees	30%	0%	25%	33%
External hacking	15%	100%	0%	13%
Accidental data loss by suppliers/organisation partners	5%	0%	0%	7%
Other, please specify	0%	0%	0%	0%
Don't know	0%	0%	0%	0%
Base	20	1	4	15

Base: Only asked of respondents who have experienced a data leakage incident

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Accidental data loss by employees	50%	75%	75%	33%	100%
Internal fraud or intentional data theft by employees	30%	0%	25%	67%	0%
External hacking	15%	25%	0%	0%	0%
Accidental data loss by suppliers/organisation partners	5%	0%	0%	0%	0%
Other, please specify	0%	0%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%
Base	20	4	4	3	1

Did the incident damage your organisation in any way?

Base: Only asked of respondents who have experienced a data leakage incident

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	55%	100%	50%	53%
No	45%	0%	50%	47%
Base	20	1	4	15

Base: Only asked of respondents who have experienced a data leakage incident

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	55%	25%	100%	33%	0%
No	45%	75%	0%	67%	100%
Base	20	4	4	3	1

Which of the following best fits the way in which the incident damaged your organisation?

Base: Only asked of respondents whose organisations have been damaged by a data leakage incident

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Reputation damage	91%	100%	100%	88%
Loss of competitive edge	27%	0%	0%	38%
Loss of suppliers/organisation partners	18%	100%	0%	13%
Loss of customers	9%	0%	0%	13%
Fines for non-compliance with regulations	9%	0%	0%	13%
Loss of my job	0%	0%	0%	0%
Other, please specify	0%	0%	0%	0%
Don't know	0%	0%	0%	0%
Base	11	1	2	8

Base: Only asked of respondents whose organisations have been damaged by a data leakage incident

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Reputation damage	91%	100%	100%	100%	0%
Loss of competitive edge	27%	0%	0%	100%	0%
Loss of suppliers/organisation partners	18%	0%	0%	0%	0%
Loss of customers	9%	0%	0%	0%	0%
Fines for non-compliance with regulations	9%	0%	0%	0%	0%
Loss of my job	0%	0%	0%	0%	0%
Other, please specify	0%	0%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%
Base	11	1	4	1	0

If possible, please quantify how much the incident damaged your organisation:

Base: (11) Only asked of respondents whose organisations have been damaged by a data leakage incident

Contract penalties

Designs given to competitor. Significant loss in potential customers

Difficult to quantify

Impossible to say

Loss of reputation with key supplier

Major publicity, increasing data security costs and staff training

Massive media coverage, resulting in high scrutiny of our company by our client. As a result we have had to spent £millions on changing processes and updating systems and policy.

Reputation

Reputational only

Would not disclose (x2)

How likely do you think it would be for an incident to damage your organisation in some way?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
It would definitely damage my organisation in some way	17%	25%	7%	18%
It would be very likely to damage my organisation	18%	25%	15%	17%
It would be likely to damage my organisation	42%	39%	44%	41%
It would be unlikely to damage my organisation	17%	9%	22%	17%
It would be very unlikely to damage my organisation	6%	2%	7%	6%
It would definitely not damage my organisation	1%	0%	2%	0%
Don't know	2%	0%	2%	2%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
It would definitely damage my organisation in some way	17%	25%	15%	13%	13%
It would be very likely to damage my organisation	18%	34%	18%	7%	8%
It would be likely to damage my organisation	42%	23%	48%	53%	46%
It would be unlikely to damage my organisation	17%	9%	9%	23%	29%
It would be very unlikely to damage my organisation	6%	5%	6%	3%	4%
It would definitely not damage my organisation	1%	2%	0%	0%	0%
Don't know	2%	2%	3%	0%	0%
Base	200	44	33	30	24

Which of the technologies below do you regard as representing the greatest data leakage risk to your organisation?

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Base: All respondents				
USB sticks and similar removable storage devices	63%	59%	57%	68%
Email	52%	59%	44%	53%
Corporate laptops	35%	39%	35%	33%
Social media, such as Twitter, Facebook, Hotmail	31%	39%	31%	26%
Employee-owned smartphones, including iPhones and BlackBerrys	28%	34%	31%	23%
Employee-owned laptops	24%	32%	13%	25%
Corporate smartphones	19%	23%	13%	21%
Employee-owned iPads or other types of tablet PCs	15%	27%	9%	12%
Employee-owned PCs	15%	11%	15%	16%
Cloud computing	15%	9%	13%	18%
Other types of mobile phones, owned by	12%	7%	11%	14%
Virtualisation	11%	11%	13%	9%
Corporate iPads or other types of tablet PCs	10%	14%	11%	7%
Consumer instant messaging applications	9%	9%	11%	8%
Corporate PCs	9%	9%	13%	6%
Other types of mobile phones, owned by the organisation	8%	9%	4%	10%
Corporate instant messaging applications	7%	9%	6%	7%
*Other, please specify	2%	2%	2%	2%
Base	200	44	54	102

*Other, please specify: "(i) Enterprise collaboration tools in the cloud, (ii) "Users", "Employees", "Hard Copy Reports", "Physical filing".

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Base: All respondents					
USB sticks and similar removable storage devices	63%	50%	73%	63%	75%
Email	52%	52%	64%	53%	46%
Corporate laptops	35%	20%	52%	30%	38%
Social media, such as Twitter, Facebook, Hotmail	31%	34%	18%	37%	42%
Employee-owned smartphones, including iPhones and BlackBerrys	28%	25%	27%	17%	29%
Employee-owned laptops	24%	18%	27%	20%	17%
Corporate smartphones	19%	11%	24%	27%	17%
Employee-owned iPads or other types of tablet PCs	15%	18%	9%	17%	13%
Employee-owned PCs	15%	16%	12%	7%	8%
Cloud computing	15%	18%	3%	7%	17%
Other types of mobile phones, owned by employees	12%	9%	9%	20%	13%
Virtualisation	11%	16%	3%	17%	4%
Corporate iPads or other types of tablet PCs	10%	14%	3%	7%	8%
Consumer instant messaging applications	9%	16%	6%	3%	8%
Corporate PCs	9%	14%	6%	10%	4%
Other types of mobile phones, owned by the organisation	8%	5%	6%	10%	13%
Corporate instant messaging applications	7%	11%	0%	10%	8%
Other, please specify	2%	5%	3%	0%	4%
Base	200	44	33	30	24

What type of data leakage threat are you most concerned about?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Accidental data loss by employees	52%	36%	56%	57%
Internal fraud or intentional data theft by employees (e.g. like the recent WikiLeaks events)	32%	41%	30%	29%
External hacking	12%	18%	9%	10%
Accidental data loss by suppliers/organisation partners	3%	2%	4%	3%
Other, please specify	0%	0%	0%	0%
Don't know	2%	2%	2%	1%
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Accidental data loss by employees	52%	43%	79%	50%	75%
Internal fraud or intentional data theft by employees (e.g. like the recent WikiLeaks events)	32%	36%	9%	43%	25%
External hacking	12%	9%	9%	3%	0%
Accidental data loss by suppliers/organisation partners	3%	9%	0%	3%	0%
Other, please specify	0%	0%	0%	0%	0%
Don't know	2%	2%	3%	0%	0%
Base	200	44	33	30	24

What are you most worried about in terms of damage from a data leak incident?

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Reputation damage	46%	30%	44%	53%
Loss of competitive edge (e.g. through loss of IP)	19%	39%	15%	13%
Loss of customers	14%	18%	15%	12%
Fines for non-compliance with regulations	13%	2%	13%	18%
Loss of suppliers/organisation partners	5%	2%	11%	3%
Loss of my job	2%	7%	0%	0%
*Other, please specify	1%	2%	0%	1%
Don't know	1%	0%	2%	1%
Base	200	44	54	102

*Other, please specify: "Confidentiality breaches", "Most of the above".

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Reputation damage	46%	50%	70%	37%	46%
Loss of competitive edge (e.g. through loss of IP)	19%	23%	3%	13%	8%
Loss of customers	14%	11%	0%	27%	13%
Fines for non-compliance with regulations	13%	7%	21%	20%	8%
Loss of suppliers/organisation partners	5%	7%	0%	3%	17%
Loss of my job	2%	0%	3%	0%	4%
Other, please specify	1%	0%	0%	0%	4%
Don't know	1%	2%	3%	0%	0%
Base	200	44	33	30	24

To what extent do you agree with the following statement? "Opening up corporate data to employees to support mobility and productivity significantly increases the risk of serious/damaging data leakage incidents."

Base: All respondents	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
5 - Totally agree	26%	48%	20%	19%
4 - Somewhat agree	56%	43%	57%	60%
3 - Neither agree nor disagree	12%	5%	15%	13%
2 - Somewhat disagree	7%	5%	6%	8%
1 - Totally disagree	0%	0%	0%	0%
Don't know	1%	0%	2%	1%
Average	4.01	4.34	3.94	3.90
Base	200	44	54	102

Base: All respondents	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
5 - Totally agree	26%	34%	18%	20%	17%
4 - Somewhat agree	56%	48%	67%	53%	58%
3 - Neither agree nor disagree	12%	11%	3%	10%	21%
2 - Somewhat disagree	7%	5%	9%	17%	4%
1 - Totally disagree	0%	0%	0%	0%	0%
Don't know	1%	2%	3%	0%	0%
Average	4.01	4.14	3.97	3.77	3.88
Base	200	44	33	30	24

To what extent do you agree with the following statement? “The use of employee-owned devices at work significantly increases the risk of serious/damaging data leakage incidents.”

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Base: All respondents				
5 - Totally agree	42%	48%	39%	41%
4 - Somewhat agree	42%	45%	48%	36%
3 - Neither agree nor disagree	12%	7%	11%	14%
2 - Somewhat disagree	3%	0%	2%	5%
1 - Totally disagree	1%	0%	0%	2%
Don't know	1%	0%	0%	2%
Average	4.22	4.41	4.24	4.12
Base	200	44	54	102

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Base: All respondents					
5 - Totally agree	42%	41%	39%	40%	42%
4 - Somewhat agree	42%	34%	52%	40%	42%
3 - Neither agree nor disagree	12%	16%	3%	13%	17%
2 - Somewhat disagree	3%	5%	6%	3%	0%
1 - Totally disagree	1%	2%	0%	0%	0%
Don't know	1%	2%	0%	3%	0%
Average	4.22	4.09	4.24	4.21	4.25
Base	200	44	33	30	24

To what extent do you agree with the following statement? “The WikiLeaks data leak and associated events has made me take a closer look at DLP solutions.”

Base: All respondents				
	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
5 - Totally agree	13%	27%	9%	9%
4 - Somewhat agree	27%	30%	28%	25%
3 - Neither agree nor disagree	35%	30%	31%	39%
2 - Somewhat disagree	12%	7%	9%	15%
1 - Totally disagree	12%	7%	19%	10%
Don't know	3%	0%	4%	3%
Average	3.18	3.64	3.00	3.08
Base	200	44	54	102

Base: All respondents					
	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
5 - Totally agree	13%	20%	6%	7%	8%
4 - Somewhat agree	27%	20%	24%	37%	17%
3 - Neither agree nor disagree	35%	30%	36%	30%	67%
2 - Somewhat disagree	12%	9%	12%	17%	4%
1 - Totally disagree	12%	18%	18%	10%	4%
Don't know	3%	2%	3%	0%	0%
Average	3.18	3.16	2.88	3.13	3.21
Base	200	44	33	30	24

Do you think your organisation has experienced a leakage of sensitive/confidential/valuable information that you are not aware of?

Base: All respondents

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	51%	39%	52%	55%
No	50%	61%	48%	45%
Base	200	44	54	102

Base: All respondents

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	51%	43%	42%	57%	54%
No	50%	57%	58%	43%	46%
Base	200	44	33	30	24

Do you think it may have damaged your organisation?

Base: Only asked of respondents who think their organisation has experienced a loss of sensitive information that they are not aware of

	Total	500 - 1000 employees	1000 - 3000 employees	More than 3000 employees
Yes	52%	71%	57%	45%
No	48%	29%	43%	55%
Base	101	17	28	56

Base: Only asked of respondents who think their organisation has experienced a loss of sensitive information that they are not aware of

	Total	Financial services	Public sector and not for profit	Retail, distribution and transport	Business and professional services
Yes	52%	47%	43%	41%	54%
No	48%	53%	57%	59%	46%
Base	101	19	14	17	13



In what way might your organisation have been damaged?

Base: (53) Only asked of respondents who think their organisation has experienced a loss of sensitive information that they are not aware of and think the organisation may have been damaged as a result

Bad publicity

Brand

clients become more careful dealing with us

Confidential information leaked points at sloppy procedures

Competitive edge. Designs are extremely sensitive and useful for competitors

Disclosing commercial information to competitors, or client customer data being used by employees for their own selfish gain.

Fraud

Hack fight

Legal fines

Looks careless and unprofessional.

Loss of business confidence in our organisation and negativity associated with our enterprise

Loss of clients to competitors (x2)

Loss of company confidential data (x2)

Loss of competitive edge (x11)

Loss of competitive edge, potential malicious damage to reputation

Loss of customer data

Loss of data protection of customers

Loss of IP (x9)

Loss of patient data would lead to mistrust and lack of confidence

Loss of profits

Loss of reputation (x6)

political reputation

Potential for reputation impact, loss of credibility

Reputation, loss of significant deals, use of public information (was confidential) by competitors in sales cycles. Open source community loss of faith.

Staff leaving and taking competitive product or customer information

Suppliers have access to the system and when mistakes happen and they can see each other's contracts as has happened, this obviously causes problems for competition in tendering.

Would not disclose (x5)