SentinelOne: Global Ransomware Study 2018

Ransomware Attacks

This year, approaching six in ten (56%) surveyed decision makers from IT and risk, fraud or compliance functions report that their organisation has suffered a ransomware attack in the last 12 months, compared to under half (48%) who said the same in 2016. Of those whose organisation has suffered a ransomware attack in the last 12 months, they have had to defend against five ransomware attacks during this period, on average.

According to almost seven in ten (69%) respondents, the most successful ransomware attack resulted in the attacker being able to encrypt some files/data, with 5% paying the ransom to decrypt the data. Of those whose organisation has suffered a ransomware attack in the last 12 months, 69% say that the ransomware attacker was able to gain access to their organisation's network by phishing via email or social media network. Around two in five report that access was gained by a drive-by-download caused by clicking on a compromised website (44%) and/or an infection via a computer that was part of a botnet (42%). The type of devices/systems most likely to be impacted by the ransomware attack(s) are desktop PCs (80%), servers (57%) and mobile devices (38%) (sheet 3), while the types of data that are most likely to have been affected in the past 12 months were employee (45%), customer (38%) and product (37%) information.

Upon suffering a ransomware attack, 5% of respondents say that the IT security department would do/did nothing. Around half report that they did/would notify the CEO/board (53%), inform law enforcement (49%) and/or notify data protection regulators (45%).

According to around half of respondents whose organisation has suffered a ransomware attack in the last 12 months, the ransomware attack was successful because an employee was careless (51%) and/or anti-virus was in place but it did not stop the ransomware attack (45%). Almost all (94%) cite that there has been some impact on their organisation because of ransomware attacks in the past 12 months, with the greatest impacts being an increased spending on IT security (67%) and a change of IT security strategy, to focus on mitigation (44%). Furthermore, more than one in ten report that their organisation has received negative press/bad publicity (14%) and/or seen senior IT staff lose their jobs (14%).

Ransomware Attacks

Nearly three in four (72%) surveyed decision makers agree that organisations are turning to cyber insurance now that the possibility of fines is higher with the GDPR and over half (52%) say that their organisation has lost faith in traditional cyber security, such as anti-virus.

This year, the average estimated number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files amounts to 40 hours, according to respondents from organisations where the most successful ransomware attack resulted in the attacker being able to encrypt some files/data. This has increased from 33 hours, which was the average estimated number reported by respondents in 2016.

Of those whose organisation has suffered a ransomware attack in the last 12 months, the average estimated business cost as a result of the ransomware attack(s) is £591,238. Furthermore, only around a third (34%) of respondents report that their organisation's third party suppliers or partners were not affected by the attack, while 40% suffered downtime as a result.

When considering all the ransomware attacks that their organisation has experienced in the last 12 months, less than half (46%) of respondents say that their organisation did not pay a ransom because they decrypted the data themselves/had backups. In contrast, around one in five (19%) admit that their organisation paid the ransom demanded by the attacker every time.

According to respondents whose organisation/the organisation's insurer has paid some or all of the ransom(s) demanded by ransomware attackers for an attack in the last 12 months, the total value of the ransoms paid in this period is £34,845, on average and the largest value that their organisation has ever paid is £34,514, on average. Nearly six in ten (58%) report that even though their organisation paid the ransom, the extortionist tried to extort a second ransom after receiving the first payment and around four in ten (42%) say that the extortionist did not decrypt the affected files despite receiving the payment.

Ransomware Attacks

Of those whose organisation/the organisation's insurer has paid some or all of the ransom(s) demanded by ransomware attackers in the last 12 months, around six in ten state that their organisation paid the ransom because the cost of paying the ransomware was less than the lost productivity caused by downtime from the attack (58%) and/or the cost of paying the ransom outweighed the cost of restoration/damage to business (56%). On the other hand, according to respondents whose organisation did not pay the ransomware attackers for an attack in the last 12 months, the most common reasons for not doing so are that they did not need to as they had back-ups/were able to decrypt themselves (51%) and because it is their organisation’s policy not to pay ransoms, saying that on ethical grounds they do not pay criminals (43%).

The clear majority (97%) of respondents that are from organisations that have suffered a ransomware attack in the last 12 months say that their organisation had back-ups for their files when thinking about the most successful ransomware attack. A third (33%) report that an employee has paid a ransom in the past without the involvement or sanction of IT/security departments.

Over three in four (76%) respondents whose organisation has suffered a ransomware attack in the last 12 months have been able to determine the identity of the attacker(s) involved, with the most likely attacker being organised cyber-criminals (53%). Of those whose organisation has been able to identify the attacker in any of the ransomware attacks on their organisation, the vast majority (94%) say that their organisation was able to determine the source of the breach, with four in ten (40%) reporting that the attack originated within their own country.

The most likely motives for cyber-attackers when using ransomware against respondents’ organisations, according to those who have suffered an attack within the last 12 months, are financial gain (62%), simple disruption to a successful business (38%) and cyber espionage (31%). Three quarters (75%) of respondents agree that behaviour based analytics is the only way to catch more complex ransomware attacks.

Data Summary – March 8th, 2018

1	Has your organisation suffered a ransomware attack in the last 12 months (whether it was successful or unsuccessful)?
2	How did the ransomware attacker gain access to your organisation's network?
3	Which of the following types of devices/systems were impacted in the ransomware attack(s) suffered by your organisation?
4	In the past 12 months, how many ransomware attacks has your organisation had to defend against?
5	How far did the most successful ransomware attack get when targeting your organisation's data?
6	When thinking about the most successful ransomware attack, did your organisation have back-ups for your files?
7	In your opinion, why was the ransomware attack on your organisation successful?
8	In terms of the business cost, what would you estimate the total cost of the ransomware attack(s) to be, that your organisation has experienced in the last 12 months?
9	Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files:
10	Considering all the ransomware attacks your organisation has experienced in the last 12 months, has your organisation paid the ransom demanded by ransomware attackers?
11	What was the total value of the ransoms paid by your organisation over the last 12 months?
12	What was the value of the largest ransom your organisation has paid?
13	What results have your organisation experienced from paying the ransom?
14	Why did your organisation decide to pay the ransom?
15	What were the reasons for your organisation not paying the ransom?
16	To your knowledge have any employees ever paid a ransom without the involvement or sanction of IT/security departments?
17	Were any of your organisation's third party suppliers or partners also affected by your ransomware attack(s)?
18	What has been the impact of ransomware attacks on your organisation in the past 12 months?
18	What type of data has been affected by ransomware attackers in the past 12 months in your organisation?
20	Upon suffering a ransomware attack, which of the following did/would your IT security department do?
21	Has your organisation been able to identify the attacker in any of the ransomware attacks on your organisation, and if so who was the attacker?
22	What do you believe to be the main motive for cyber-attackers when using ransomware against your organisation?
23	Was your organisation able to locate the origin of the ransomware attacker(s)/the location of the attacker(s)?
Demographics	
D1	How many employees does your organisation have globally?
D2	Within which sector is your organisation?
D3	In which one of these functional areas are you primarily employed within your organisation?
D4	What is your level of involvement in IT security within your organisation?

Has your organization suffered a ransomware attack in the last 12 months (whether it was successful or unsuccessful)?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Yes	56%	40%	55%	59%	70%	59%	62%	45%
No	43%	56%	43%	41%	30%	41%	38%	50%
Don’t know	2%	4%	2%	0%	0%	0%	1%	5%

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Yes	56%	63%	65%	65%	49%	67%	42%	36%	59%	62%
No	43%	33%	35%	35%	49%	33%	56%	59%	40%	38%
Don’t know	2%	3%	0%	0%	2%	0%	2%	5%	2%	0%

How did the ransomware attacker gain access to your organization's network?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Phishing via email or social media network	69%	70%	70%	58%	76%	66%	66%	78%
Drive-by-download caused by clicking on a compromised website	44%	38%	52%	42%	36%	44%	51%	31%
Infection via a computer that was part of a botnet	42%	15%	45%	39%	56%	43%	48%	29%
Infection via a worm that spread laterally across the network	27%	10%	37%	24%	23%	23%	38%	14%
*Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	1%	3%	0%	2%	0%	1%	0%	1%

How did the ransomware attacker gain access to your organization's network?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilites	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Phishing via email or social media network	69%	55%	55%	82%	86%	69%	52%	79%	71%	72%
Drive-by-download caused by clicking on a compromised website	44%	55%	36%	45%	31%	50%	40%	29%	44%	44%
Infection via a computer that was part of a botnet	42%	45%	45%	73%	34%	61%	36%	17%	38%	28%
Infection via a worm that spread laterally across the network	27%	20%	27%	27%	24%	35%	16%	33%	32%	21%
*Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	1%	0%	0%	0%	3%	0%	0%	0%	0%	0%

Which of the following types of devices/systems were impacted in the ransomware attack(s) suffered by your organisation?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Desktop PCs	80%	73%	89%	68%	79%	80%	80%	77%
Servers	57%	35%	65%	56%	59%	53%	65%	51%
Mobile devices (laptops, tablets and mobile phones)	38%	28%	43%	31%	44%	48%	29%	38%
Connected/IoT devices such as medical devices	28%	10%	34%	27%	29%	23%	38%	17%
Cloud-based systems	22%	5%	29%	24%	19%	14%	33%	15%
SCADA systems	18%	5%	20%	24%	17%	13%	24%	15%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	0%	3%	0%	0%	0%	0%	0%	2%

Which of the following types of devices/systems were impacted in the ransomware attack(s) suffered by your organisation?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Desktop PCs	80%	83%	64%	100%	83%	76%	72%	92%	83%	72%
Servers	57%	55%	64%	73%	41%	61%	52%	63%	56%	60%
Mobile devices (laptops, tablets and mobile phones)	38%	45%	27%	45%	34%	48%	36%	8%	35%	42%
Connected/IoT devices such as medical devices	28%	15%	18%	36%	28%	52%	16%	13%	26%	21%
Cloud-based systems	22%	20%	27%	36%	24%	24%	20%	25%	15%	19%
SCADA systems	18%	10%	36%	0%	17%	34%	12%	17%	18%	7%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

In the past 12 months, how many ransomware attacks has your organization had to defend against?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
1 attack	17%	25%	16%	24%	9%	23%	13%	17%
2 attacks	20%	20%	19%	25%	16%	23%	16%	22%
3 attacks	14%	15%	12%	14%	17%	13%	16%	12%
4 attacks	11%	5%	13%	17%	7%	6%	16%	6%
5-6 attacks	12%	5%	9%	7%	24%	9%	13%	15%
7-8 attacks	10%	8%	15%	5%	7%	11%	11%	6%
9-10 attacks	6%	8%	8%	2%	6%	7%	6%	5%
11-15 attacks	4%	0%	4%	3%	7%	5%	3%	5%
16-20 attacks	5%	8%	4%	3%	6%	1%	7%	6%
More than 20 attacks (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	2%	8%	1%	0%	1%	1%	0%	6%
Average number of ransomware attacks that respondents’ organizations have had to defend against in the past 12 months	5	5	5	4	6	4	5	5

In the past 12 months, how many ransomware attacks has your organization had to defend against?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
1 attack	17%	15%	9%	18%	21%	10%	20%	29%	24%	16%
2 attacks	20%	25%	27%	27%	17%	16%	32%	17%	12%	19%
3 attacks	14%	25%	18%	9%	10%	10%	8%	17%	12%	16%
4 attacks	11%	13%	27%	0%	10%	5%	8%	13%	15%	16%
5-6 attacks	12%	5%	0%	18%	28%	11%	16%	13%	12%	7%
7-8 attacks	10%	8%	9%	27%	3%	21%	8%	4%	3%	5%
9-10 attacks	6%	5%	0%	0%	7%	13%	4%	0%	6%	5%
11-15 attacks	4%	0%	0%	0%	0%	3%	0%	0%	12%	12%
16-20 attacks	5%	3%	9%	0%	3%	8%	4%	8%	6%	0%
More than 20 attacks (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	2%	3%	0%	0%	0%	3%	0%	4%	0%	5%
Average number of ransomware Attacks that respondents' organizations have had to defend against in the past 12 months	5	4	5	4	4	6	4	4	5	5

How far did the most successful ransomware attack get when targeting your organization's data?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
The attack was not successful – the Attacker was unable to successfully encrypt any files/data	31%	43%	27%	37%	26%	26%	30%	40%
The attacker was able to encrypt some files/data, but we were able to decrypt them ourselves	34%	20%	37%	22%	47%	42%	31%	26%
The attacker was able to encrypt some files/data, but we had a back-up and were able to replace the encrypted files	25%	35%	20%	31%	21%	24%	25%	26%
The attacker was able to encrypt some files/data, which we were unable to decrypt	5%	3%	5%	7%	4%	5%	3%	8%
The attacker was able to encrypt some files/data, and we paid the ransom in order to decrypt the data	5%	0%	11%	3%	1%	3%	11%	0%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%

How far did the most successful ransomware attack get when targeting your organization's data?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
The attack was not successful – the Attacker was unable to successfully Encrypt and files/data	31%	23%	36%	9%	52%	21%	40%	33%	26%	42%
The attacker was able to encrypt some files/data, but we were able to decrypt them ourselves	34%	40%	36%	55%	24%	37%	20%	33%	29%	37%
The attacker was able to encrypt some files/data, but we had a back-up and were able to replace the encrypted files	25%	25%	9%	36%	24%	16%	32%	33%	35%	21%
The attacker was able to encrypt some files/data, which we were unable to decrypt	5%	8%	0%	0%	0%	10%	4%	0%	9%	0%
The attacker was able to encrypt some files/data, and we paid the ransom in order to decrypt the data	5%	5%	18%	0%	0%	16%	4%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

When thinking about the most successful ransomware attack, did your organisation have back-ups for your files

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Yes	97%	93%	99%	100%	96%	100%	96%	97%
No	3%	8%	1%	0%	4%	0%	4%	3%
Don’t know	0%	0%	0%	0%	0%	0%	0%	0%

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Yes	97%	98%	100%	100%	97%	98%	100%	100%	94%	95%
No	3%	3%	0%	0%	3%	2%	0%	0%	6%	5%
Don’t know	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

In your opinion, why was the ransomware attack on your organisation successful?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
An employee was careless	51%	70%	56%	34%	44%	48%	54%	48%
We had anti-virus in place but it did not stop the ransomware attack	45%	30%	53%	44%	41%	42%	48%	43%
Our response to the attack was not fast enough	30%	15%	33%	29%	36%	24%	38%	26%
We had not updated/patched systems	26%	20%	24%	31%	29%	20%	29%	29%
Our security protocols are not adhered to by all employees	22%	28%	22%	20%	19%	20%	21%	25%
We did not have anti-virus in place	7%	3%	5%	8%	13%	10%	5%	6%
We did not have the skills in-house to rectify the situation	6%	5%	6%	5%	7%	8%	5%	5%
*Other (please specify)	1%	5%	0%	0%	0%	0%	1%	2%
Don’t know	1%	0%	2%	2%	1%	1%	2%	2%

In your opinion, why was the ransomware attack on your organisation successful?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
An employee was careless	51%	40%	27%	55%	59%	63%	68%	58%	47%	30%
We had anti-virus in place but it did not stop the ransomware attack	45%	53%	45%	55%	31%	52%	24%	38%	45%	40%
Our response to the attack was not fast enough	30%	15%	55%	27%	28%	47%	16%	17%	29%	33%
We had not updated/patched systems	26%	25%	18%	9%	24%	18%	24%	29%	29%	42%
Our security protocols are not adhered to by all employees	22%	18%	18%	45%	31%	24%	24%	33%	3%	16%
We did not have anti-virus in place	7%	8%	0%	0%	0%	8%	8%	8%	6%	14%
We did not have the skills in-house to rectify the situation	6%	8%	0%	27%	0%	5%	4%	17%	6%	2%
*Other (please specify)	1%	0%	0%	0%	0%	0%	0%	8%	0%	0%
Don’t know	1%	0%	0%	0%	7%	2%	0%	0%	0%	2%

In terms of the business cost, what would you estimate the total cost of the ransomware attack(s) to be, that your organisation has experienced in the last 12 months?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
*Less than £100,000 (please specify)	11%	35%	4%	15%	4%	11%	9%	14%
£100,000-£499,999	37%	28%	43%	36%	36%	45%	31%	35%
£500,000-£999,999	25%	13%	26%	22%	34%	26%	28%	20%
£1 million-£1.5 million	18%	8%	20%	20%	17%	6%	26%	22%
**More than £1.5 million (please specify)	1%	0%	1%	0%	1%	1%	0%	2%
Don't know	8%	18%	6%	7%	7%	11%	6%	8%
Average estimated business cost as a result of the ransomware attack(s) experienced by respondents' organisations (GBP)	£591,238	£329,976	£647,702	£572,138	£651,358	£479,387	£667.985	£626,569

In terms of the business cost, what would you estimate the total cost of the ransomware attack(s) to be, that your organisation has experienced in the last 12 months?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
*Less than £100,000 (please specify)	11%	8%	0%	18%	24%	3%	12%	29%	12%	5%
£100,000-£499,999	37%	55%	64%	18%	34%	27%	28%	25%	35%	49%
£500,000-£999,999	25%	25%	27%	36%	21%	31%	28%	21%	26%	19%
£1 million-£1.5 million	18%	10%	9%	27%	14%	32%	16%	4%	18%	14%
**More than £1.5 million (please specify)	1%	3%	0%	0%	0%	0%	4%	0%	0%	0%
Don't know	8%	0%	0%	0%	7%	6%	12%	21%	9%	14%
Average estimated business cost as a result of the ransomware attack(s) experienced by respondents' organisations (GBP)	£591,238	£525,012	£509,090	£676,332	£467,748	£765,948	£711,529	£362,926	£577,525	£535,406

Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
*Less than 8 employee hours	1%	4%	1%	0%	0%	1%	0%	3%
8-16 employee hours	10%	26%	9%	3%	12%	13%	26%	19%
16-24 employee hours	8%	9%	8%	11%	8%	12%	5%	8%
24-32 employee hours	17%	13%	15%	27%	15%	20%	13%	21%
32-40 employee hours	12%	22%	10%	5%	15%	8%	21%	3%
40-48 employee hours	21%	9%	19%	24%	27%	24%	17%	23%
48-56 employee hours	10%	0%	13%	5%	15%	15%	3%	18%
56-64 employee hours	6%	4%	9%	8%	2%	5%	9%	3%
64-72 employee hours	5%	0%	6%	11%	0%	0%	8%	8%
72-80 employee hours	7%	0%	10%	5%	6%	1%	14%	3%
**More than 80 employee hours	1%	0%	1%	0%	0%	0%	0%	3%
We did not spend any time replacing or attempting to decrypt the encrypted files, we just paid the ransom	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%
Average estimated number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files	40	26	44%	42	38	35	44%	42%

Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
*Less than 8 employee hours	1%	0%	0%	0%	0%	0%	0%	13%	0%	0%
8-16 employee hours	10%	13%	0%	10%	7%	12%	13%	19%	4%	8%
16-24 employee hours	8%	6%	14%	10%	7%	2%	0%	13%	8%	24%
24-32 employee hours	17%	19%	43%	30%	36%	8%	20%	0%	20%	16%
32-40 employee hours	12%	13%	29%	0%	7%	10%	27%	0%	16%	12%
40-48 employee hours	21%	23%	14%	30%	21%	24%	20%	13%	24%	12%
48-56 employee hours	10%	6%	0%	10%	0%	16%	0%	25%	8%	12%
56-64 employee hours	6%	13%	0%	10%	0%	8%	7%	6%	0%	4%
64-72 employee hours	5%	3%	0%	0%	7%	8%	0%	0%	8%	4%
72-80 employee hours	7%	3%	0%	0%	7%	10%	13%	6%	12%	0%
More than 80 employee hours	1%	0%	0%	0%	0%	0%	0%	0%	0%	4%
We did not spend any time replacing or attempting to decrypt the encrypted files, we just paid the ransom	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	2%	0%	0%	0%	7%	0%	0%	6%	0%	4%
Average estimated number of employee hours dedicated to replacing encrypted data with back-up data or attempting to decrypt the encrypted files	40	39	31	36	37	45	40	34	43	39

Considering all the ransomware attacks your organisation has experienced in the last 12 months, has your organisation paid the ransom demanded by ransomware attackers?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Yes, my organisation paid the ransom every time	19%	0%	34%	12%	13%	19%	26%	8%
Yes, my organisation has paid some ransoms but not all	13%	3%	11%	20%	16%	19%	11%	8%
My organisation's insurer paid all/part of the ransom(s)	15%	10%	12%	22%	16%	16%	12%	18%
No ransom was paid and we lost the data	7%	5%	5%	15%	3%	9%	4%	9%
No ransom was paid because we decrypted the data ourselves/had back-ups	46%	80%	38%	31%	53%	37%	48%	57%
Don't know	1%	3%	0%	0%	0%	1%	0%	0%

Considering all the ransomware attacks your organisation has experienced in the last 12 months, has your organisation paid the ransom demanded by ransomware attackers?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Yes, my organisation paid the ransom every time	19%	15%	9%	9%	17%	40%	8%	4%	9%	21%
Yes, my organisation has paid some ransoms but not all	13%	10%	18%	27%	7%	15%	8%	8%	18%	14%
My organisation's insurer paid all/part of the ransom(s)	15%	13%	45%	36%	7%	10%	20%	8%	12%	19%
No ransom was paid and we lost the data	7%	18%	0%	9%	3%	0%	12%	4%	12%	5%
No ransom was paid because we decrypted the data ourselves/had back-ups	46%	45%	27%	18%	66%	35%	52%	75%	50%	40%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%

What was the total value of the ransoms paid by your organisation over the last 12 months?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Less than £500 (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
£500-£999	6%	0%	5%	13%	3%	9%	4%	5%
£1,000-£4,999	3%	0%	5%	0%	3%	6%	0%	5%
£5,000-£9,999	7%	0%	3%	16%	6%	6%	7%	9%
£10,000-£19,999	17%	20%	16%	22%	13%	22%	15%	9%
£20,000-£29,999	13%	20%	6%	9%	29%	17%	13%	5%
£30,000-£39,999	15%	40%	15%	13%	16%	20%	7%	23%
£40,000-£49,999	15%	0%	19%	6%	19%	11%	19%	18%
£50,000-£99,999	20%	0%	29%	16%	10%	7%	31%	23%
£100,000 or more (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	3%	20%	2%	6%	0%	2%	4%	5%
Average value of the ransom(s) paid by respondents' organisations (GBP)	£34,845	£27,500	£40,676	£27,516	£31,411	£26,325	£42,144	£38,273

What was the total value of the ransoms paid by your organisation over the last 12 months?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Less than £500 (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
£500-£999	6%	7%	0%	0%	0%	5%	11%	20%	8%	9%
£1,000-£4,999	3%	7%	13%	0%	0%	0%	11%	0%	0%	4%
£5,000-£9,999	7%	7%	13%	13%	11%	5%	0%	0%	8%	9%
£10,000-£19,999	17%	20%	38%	38%	0%	13%	11%	20%	15%	17%
£20,000-£29,999	13%	7%	25%	0%	22%	5%	22%	0%	8%	30%
£30,000-£39,999	15%	13%	13%	25%	11%	15%	0%	20%	23%	17%
£40,000-£49,999	15%	33%	0%	13%	33%	20%	22%	0%	0%	4%
£50,000-£99,999	20%	0%	0%	13%	11%	38%	22%	40%	23%	9%
£100,000 or more (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	3%	7%	0%	0%	11%	0%	0%	0%	15%	0%
Average value of the ransom(s) paid by respondents' organisations (GBP)	£34,845	£26,875	£17,562	£30,312	£37,812	£45,912	£34,305	£40,150	£35,750	£25,630

What was the value of the largest ransom your organisation has paid?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Less than £500 (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
£500-£999	5%	0%	3%	13%	3%	7%	4%	5%
£1,000-£4,999	2%	0%	3%	0%	3%	4%	2%	0%
£5,000-£9,999	8%	0%	8%	13%	3%	9%	6%	9%
£10,000-£19,999	15%	20%	11%	16%	19%	15%	15%	14%
£20,000-£29,999	17%	20%	13%	16%	26%	24%	13%	9%
£30,000-£39,999	16%	20%	13%	22%	16%	17%	15%	18%
£40,000-£49,999	15%	20%	15%	9%	19%	15%	13%	18%
£50,000-£99,999	18%	0%	32%	6%	6%	6%	31%	18%
£100,000 or more (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	4%	20%	2%	6%	3%	4%	2%	9%
Average value of the largest ransom that respondents' organisations have paid (GBP)	£34,514	£30,000	£41,557	£25,433	£29,875	£26,759	£41,358	£36,537

What was the value of the largest ransom your organisation has paid?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Less than £500 (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
£500-£999	5%	7%	0%	0%	0%	5%	11%	0%	8%	9%
£1,000-£4,999	2%	7%	0%	0%	0%	0%	0%	0%	8%	4%
£5,000-£9,999	8%	0%	38%	13%	0%	5%	11%	0%	8%	9%
£10,000-£19,999	15%	7%	25%	13%	11%	20%	11%	40%	8%	9%
£20,000-£29,999	17%	33%	13%	13%	11%	10%	0%	20%	23%	26%
£30,000-£39,999	16%	20%	25%	13%	44%	15%	11%	0%	15%	9%
£40,000-£49,999	15%	20%	0%	13%	11%	20%	11%	40%	8%	9%
£50,000-£99,999	18%	0%	0%	25%	11%	38%	22%	0%	15%	9%
£100,000 or more (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	4%	7%	0%	13%	11%	0%	11%	0%	8%	0%
Average value of the ransom that respondents' organisations have paid (GBP)	£34,845	£27,410	£18,437	£39,642	£37,500	£46,412	£33,531	£29,000	£30,520	£24,760

What results have your organisation experienced from paying the ransom?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
The extortionist tried to extort a second ransom after receiving the first payment	58%	40%	73%	47%	45%	57%	65%	45%
The extortionist did not decrypt the affected files despite receiving the payment	42%	60%	29%	47%	61%	39%	44%	45%
The extortionist released confidential data after the ransom had been paid	38%	40%	47%	28%	32%	37%	44%	27%
The extortionist decrypted the affected files and left our network	20%	0%	26%	19%	13%	20%	22%	14%
Don’t know	2%	20%	2%	0%	0%	2%	2%	0%

What results have your organisation experienced from paying the ransom?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
The extortionist tried to extort a second ransom after receiving the first payment	58%	53%	38%	63%	56%	73%	22%	100%	46%	57%
The extortionist did not decrypt the affected files despite receiving the payment	42%	67%	63%	50%	33%	30%	33%	20%	54%	43%
The extortionist released confidential data after the ransom had been paid	38%	33%	0%	25%	22%	55%	33%	0%	54%	39%
The extortionist decrypted the affected files and left our network	20%	7%	25%	25%	11%	28%	11%	0%	15%	26%
Don’t know	2%	0%	0%	0%	11%	0%	11%	0%	0%	0%

Why did your organisation decide to pay the ransom?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
The cost of paying the ransomware was less than the lost productivity caused by downtime from the attack	58%	60%	63%	47%	61%	65%	57%	45%
The cost of paying the ransom outweighed the cost of restoration/damage to business	56%	20%	65%	53%	48%	50%	67%	45%
We wanted a quick resolution to the situation	27%	20%	35%	28%	10%	26%	28%	27%
No back-ups of data – payment was the only way to get our data back	0%	0%	0%	0%	0%	0%	0%	0%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	2%	40%	0%	3%	0%	4%	2%	0%

Why did your organisation decide to pay the ransom?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
The cost of paying the ransomware was less than the lost productivity caused by downtime from the attack	58%	53%	75%	38%	44%	68%	56%	0%	77%	57%
The cost of paying the ransom outweighed the cost of restoration/damage to business	56%	47%	25%	63%	67%	73%	22%	60%	23%	70%
We wanted a quick resolution to the situation	27%	13%	25%	38%	0%	40%	22%	40%	23%	22%
No back-ups of data – payment was the only way to get our data back	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	2%	7%	0%	0%	11%	0%	11%	0%	0%	0%

What were the reasons for your organisation not paying the ransom?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
We did not need to as we had back-ups/were able to decrypt ourselves	51%	62%	52%	37%	49%	49%	57%	44%
It is the organisation's policy not to pay ransoms/on ethical grounds we do not pay criminals	43%	56%	42%	33%	38%	40%	31%	60%
There is no guarantee of getting files back	36%	44%	44%	15%	33%	32%	40%	35%
We did not want to appear easy to extort money from	30%	29%	35%	30%	26%	32%	24%	37%
It would cost more to pay the ransom than it would to restore back-ups	26%	32%	29%	22%	21%	30%	22%	28%
We did not have the means to pay the ransom	1%	0%	2%	4%	0%	2%	0%	2%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	1%	0%	2%	0%	0%	0%	0%	2%

What were the reasons for your organisation not paying the ransom?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
We did not need to as we had back-ups/were able to decrypt ourselves	51%	44%	33%	67%	50%	59%	63%	42%	48%	53%
It is the organisation's policy not to pay ransoms/on ethical grounds we do not pay criminals	43%	32%	33%	100%	50%	50%	31%	47%	38%	42%
There is no guarantee of getting files back	36%	48%	0%	0%	35%	27%	25%	37%	52%	32%
We did not want to appear easy to extort money from	30%	40%	33%	33%	30%	23%	13%	21%	38%	42%
It would cost more to pay the ransom than it would to restore back-ups	26%	28%	33%	33%	30%	27%	25%	26%	24%	21%
We did not have the means to pay the ransom	1%	0%	0%	0%	0%	5%	0%	0%	0%	5%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	1%	0%	0%	0%	0%	0%	0%	0%	0%	5%

To your knowledge have any employees ever paid a ransom without the involvement or sanction of IT/security departments?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Yes	33%	0%	44%	39%	29%	36%	37%	20%
No	60%	78%	55%	54%	64%	56%	61%	66%
Don't know	7%	23%	2%	7%	7%	8%	3%	14%

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Yes	33%	25%	36%	36%	21%	65%	8%	13%	24%	33%
No	60%	70%	55%	64%	72%	34%	88%	67%	65%	58%
Don't know	7%	5%	9%	0%	7%	2%	4%	21%	12%	9%

Were any of your organisation's third party suppliers or partners also affected by your ransomware attack(s)?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Yes, they suffered downtime	40%	18%	46%	47%	36%			
Yes, they suffered a loss in productivity	33%	15%	35%	37%	39%			
Yes, they suffered a loss of revenue	17%	13%	20%	20%	11%			
No, they were not affected by the ransomware attack	34%	68%	34%	15%	33%			
Don't know	5%	5%	4%	7%	4%			

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Yes, they suffered downtime	40%	43%	45%	45%	24%	52%	36%	33%	35%	37%
Yes, they suffered a loss in productivity	33%	23%	27%	45%	28%	42%	28%	17%	38%	42%
Yes, they suffered a loss of revenue	17%	10%	45%	36%	7%	21%	16%	13%	24%	9%
No, they were not affected by the ransomware attack	34%	43%	18%	36%	38%	27%	40%	54%	26%	30%
Don't know	5%	8%	0%	0%	10%	3%	0%	0%	12%	2%

What has been the impact of ransomware attacks on your organization in the past 12 months?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Increased spending on IT security	67%	58%	75%	54%	71%	73%	62%	68%
Change of IT security strategy, to focus on mitigation	44%	45%	50%	34%	44%	47%	46%	38%
Loss of confidence in existing cybersecurity solutions	29%	20%	30%	32%	29%	25%	33%	28%
Damage to company reputation	25%	5%	30%	34%	21%	26%	22%	28%
My organization invested in cyber insurance	23%	15%	25%	19%	29%	23%	22%	26%
Negative press/bad publicity	14%	13%	10%	20%	17%	8%	16%	22%
Senior IT staff (CIO, CISO) lost their jobs	14%	8%	21%	8%	13%	12%	18%	12%
*Other (please specify)	0%	0%	0%	0%	0%	0%	0%	2%
There was no impact on my organization because of ransomware attacks in the past12 months	6%	28%	3%	0%	4%	3%	7%	9%

What has been the impact of ransomware attacks on your organization in the past 12 months?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Increased spending on IT security	67%	78%	36%	73%	62%	61%	76%	63%	71%	70%
Change of IT security strategy, to focus on mitigation	44%	30%	27%	73%	45%	56%	32%	50%	38%	47%
Loss of confidence in existing cybersecurity solutions	29%	33%	36%	18%	28%	23%	24%	25%	44%	28%
Damage to company reputation	25%	23%	45%	27%	24%	35%	12%	25%	18%	21%
My organization invested in cyber insurance	23%	25%	18%	36%	17%	27%	36%	8%	21%	21%
Negative press/bad publicity	14%	8%	36%	27%	10%	8%	16%	21%	18%	16%
Senior IT staff (CIO, CISO) lost their jobs	14%	5%	9%	9%	17%	32%	12%	8%	9%	7%
*Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%
There was no impact on my organization because of ransomware attacks in the past12 months	6%	3%	9%	0%	7%	8%	4%	13%	6%	5%

What type of data has been affected by ransomware attackers in the past 12 months in your organization?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Employee information	45%	23%	60%	29%	49%	54%	44%	34%
Customer information	38%	15%	47%	44%	31%	41%	37%	35%
Product information	37%	30%	39%	32%	41%	38%	39%	31%
Financial data	35%	15%	38%	46%	31%	34%	35%	35%
Payroll/HR	22%	5%	26%	25%	23%	26%	21%	18%
Research and design	21%	18%	21%	17%	27%	23%	21%	18%
Company IP	14%	15%	17%	5%	14%	10%	19%	11%
All data was targeted	7%	18%	7%	7%	1%	6%	7%	9%
Don’t know	4%	10%	3%	7%	1%	3%	4%	6%

What type of data has been affected by ransomware attackers in the past 12 months in your organization?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Employee information	45%	35%	36%	45%	34%	65%	36%	42%	38%	49%
Customer information	38%	43%	36%	27%	34%	39%	28%	25%	59%	35%
Product information	37%	25%	55%	27%	31%	44%	48%	29%	35%	40%
Financial data	35%	43%	55%	27%	34%	39%	16%	25%	35%	35%
Payroll/HR	22%	25%	27%	9%	14%	32%	0%	17%	29%	23%
Research and design	21%	13%	45%	36%	28%	21%	28%	17%	15%	19%
Company IP	14%	5%	0%	9%	7%	5%	8%	25%	6%	5%
All data was targeted	7%	5%	0%	9%	7%	5%	8%	25%	6%	5%
Don’t know	4%	5%	0%	9%	3%	5%	0%	8%	3%	5%

Upon suffering a ransomware attack, which of the following did/would your IT security department do?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Notify the CEO/board	53%	62%	55%	42%	50%	50%	48%	61%
Inform law enforcement	49%	45%	54%	50%	44%	51%	45%	53%
Notify data protection regulators (e.g. ICO)	45%	46%	48%	35%	48%	44%	43%	48%
Attempt to decrypt the files ourselves	42%	31%	45%	44%	48%	44%	40%	44%
Demand answers from IT security vendor/consultant	36%	30%	37%	35%	42%	30%	38%	40%
Notify our lawyers	35%	38%	36%	33%	32%	35%	33%	38%
Notify customers	31%	23%	37%	32%	28%	32%	28%	35%
Contact our cyber insurance provider	24%	11%	29%	26%	24%	27%	21%	24%
Change IT security vendor/consultant	17%	8%	22%	14%	19%	18%	18%	14%
*Other (please specify)	1%	2%	1%	0%	1%	1%	1%	1%
None of the above	5%	16%	4%	1%	1%	4%	5%	6%

Upon suffering a ransomware attack, which of the following did/would your IT security department do?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Notify the CEO/board	53%	51%	41%	47%	63%	48%	63%	50%	52%	51%
Inform law enforcement	49%	46%	47%	59%	47%	55%	56%	52%	40%	45%
Notify data protection regulators (e.g. ICO)	45%	52%	29%	65%	42%	51%	46%	42%	41%	35%
Attempt to decrypt the files ourselves	42%	46%	29%	41%	39%	47%	41%	38%	50%	39%
Demand answers from IT security vendor/consultant	36%	30%	24%	24%	36%	38%	51%	38%	40%	29%
Notify our lawyers	35%	35%	41%	47%	39%	37%	42%	27%	24%	35%
Notify customers	31%	27%	53%	24%	17%	32%	29%	32%	34%	42%
Contact our cyber insurance provider	24%	17%	24%	29%	24%	23%	29%	24%	17%	30%
Change IT security vendor/consultant	17%	8%	12%	18%	15%	29%	27%	12%	12%	12%
*Other (please specify)	1%	0%	0%	6%	0%	0%	2%	2%	2%	0%
None of the above	5%	3%	6%	0%	3%	2%	3%	11%	7%	7%

Has your organization been able to identify the attacker in any of the ransomware attacks on your organization, and if so who was the attacker?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Organised cyber-criminals	53%	30%	59%	58%	51%	56%	48%	55%
Political hacktivists	25%	10%	27%	27%	30%	23%	29%	23%
Dissatisfied customers	23%	10%	24%	20%	30%	25%	26%	12%
Rival organisations	20%	10%	25%	7%	29%	19%	26%	12%
Disgruntled employees/former employees	15%	10%	17%	15%	16%	15%	18%	12%
State sponsored hackers	11%	10%	18%	3%	6%	11%	12%	6%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
My organisation has not been able to determine the identity of the attacker in any of the ransomware attacks we have suffered	24%	53%	22%	17%	19%	25%	24%	23%

Has your organization been able to identify the attacker in any of the ransomware attacks on your organization, and if so who was the attacker?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Organised cyber-criminals	53%	65%	45%	64%	52%	63%	40%	29%	47%	51%
Political hacktivists	25%	33%	36%	18%	21%	32%	8%	8%	32%	26%
Dissatisfied customers	23%	20%	27%	36%	21%	34%	12%	0%	21%	19%
Rival organisations	20%	13%	18%	9%	10%	32%	20%	21%	21%	19%
Disgruntled employees/former employees	15%	8%	18%	27%	17%	27%	8%	17%	12%	7%
State sponsored hackers	11%	3%	18%	9%	10%	27%	12%	8%	0%	2%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
My organisation has not been able to determine the identity of the attacker in any of the ransomware attacks we have suffered	24%	18%	27%	34%	16%	36%	63%	42%	29%	23%

What do you believe to be the main motive for cyberattackers when using ransomware against your organization?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Financial gain	62%	73%	69%	56%	51%	60%	62%	68%
Simple disruption to a successful business	38%	25%	42%	44%	34%	39%	40%	32%
Cyber espionage	31%	13%	33%	29%	41%	34%	29%	29%
Political motivation	24%	5%	29%	24%	29%	31%	21%	18%
'Revenge' for a bad experience with my organisation	21%	8%	29%	24%	13%	25%	24%	9%
State sponsored international attack	13%	20%	15%	5%	13%	11%	17%	9%
Entertainment (hacking just for fun)	10%	13%	13%	0%	11%	9%	10%	11%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
We have no insight into the motivation of the cyber-attackers targeting my organisation	6%	5%	6%	8%	6%	9%	6%	3%

What do you believe to be the main motive for cyberattackers when using ransomware against your organization?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Financial gain	62%	60%	64%	55%	76%	60%	60%	67%	59%	63%
Simple disruption to a successful business	38%	38%	27%	27%	41%	45%	28%	29%	41%	40%
Cyber espionage	31%	23%	18%	45%	34%	45%	20%	21%	35%	26%
Political motivation	24%	25%	45%	36%	17%	34%	4%	17%	21%	26%
‘Revenge’ for a bad experience with my organisation	21%	15%	18%	18%	7%	39%	16%	21%	21%	14%
State sponsored international attack	13%	10%	9%	0%	10%	19%	20%	21%	9%	7%
Entertainment (hacking just for fun)	10%	10%	9%	18%	10%	13%	12%	8%	0%	9%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
We have no insight into the motivation of the cyber-attackers targeting my organisation	6%	5%	0%	9%	0%	5%	12%	8%	9%	9%

Was your organisation able to locate the origin of the ransomware attacker(s)/the location of the attacker(s)?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Within my own country	40%	32%	51%	35%	32%	38%	41%	42%
Eastern Europe	31%	32%	21%	39%	40%	39%	26%	28%
Western Europe	25%	16%	24%	18%	33%	29%	24%	20%
North America	21%	5%	42%	8%	7%	25%	22%	14%
Middle East	13%	11%	13%	12%	14%	18%	9%	10%
Far East	9%	26%	7%	2%	14%	16%	6%	6%
Africa	9%	16%	7%	14%	4%	11%	8%	6%
South America	6%	0%	12%	4%	2%	8%	6%	4%
My organisation was unable to determine the source location of the breach	6%	16%	5%	8%	2%	7%	4%	8%

Was your organisation able to locate the origin of the ransomware attacker(s)/the location of the attacker(s)?

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
Within my own country	40%	58%	22%	38%	42%	38%	13%	43%	42%	39%
Eastern Europe	31%	22%	0%	63%	26%	29%	44%	21%	46%	36%
Western Europe	25%	11%	22%	38%	37%	33%	13%	0%	42%	21%
North America	21%	17%	22%	50%	16%	42%	13%	7%	8%	9%
Middle East	13%	11%	11%	13%	11%	19%	6%	7%	17%	9%
Far East	9%	8%	0%	25%	11%	6%	13%	14%	8%	12%
Africa	9%	6%	22%	13%	0%	12%	6%	0%	13%	9%
South America	6%	8%	0%	13%	0%	15%	0%	0%	0%	3%
My organisation was unable to determine the source location of the breach	6%	8%	11%	13%	11%	2%	6%	7%	4%	3%

How many employees does your organisation have globally?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
1,001-3,000 employees	35%	21%	38%	39%	38%			
3,001-5,000 employees	36%	36%	37%	35%	37%			
More than 5,000 employees	29%	43%	25%	26%	25%			

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
1,001-3,000 employees	35%	38%	47%	59%	17%	37%	42%	32%	28%	38%
3,001-5,000 employees	36%	40%	41%	29%	51%	41%	20%	26%	50%	28%
More than 5,000 employees	29%	22%	12%	12%	32%	22%	37%	42%	22%	35%

Within which sector is your organisation?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
IT, technology and telecoms	18%	11%	21%	18%	22%	20%	21%	14%
Public sector	13%	19%	17%	8%	5%	12%	9%	19%
Business and professional services	13%	10%	11%	18%	14%	14%	14%	10%
Financial services	12%	19%	9%	7%	15%	6%	16%	13%
Manufacturing and production	12%	12%	10%	10%	18%	14%	7%	15%
Retail, distribution and transport	12%	14%	10%	15%	9%	9%	16%	9%
Construction and property	3%	1%	3%	8%	3%	5%	4%	1%
Energy, oil/gas and utilities	3%	2%	5%	2%	3%	6%	3%	1%
*Other commercial sector (please specify)	14%	12%	16%	14%	11%	15%	10%	17%

In which one of these functional areas are you primarily employed within your organisation?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
Information technology	91%	100%	87%	87%	93%	90%	92%	91%
Risk/fraud/compliance/governance	9%	0%	13%	13%	7%	10%	8%	9%

What is your level of involvement in IT security within your organisation?

	Total	UK	US	France	Germany	1-3K employees	3-5K employees	5K+ employees
I work exclusively in IT security	39%	17%	45%	47%	42%	47%	43%	26%
The majority of my work involves IT security	31%	23%	24%	41%	42%	30%	35%	26%
Some of my work involves IT security but I have other responsibilities	30%	60%	32%	12%	16%	24%	22%	49%

	Total	Business and professional services	Construction and property	Energy, oil/gas and utilities	Financial services	IT, technology and telecoms	Manufacturing and production	Public sector	Retail distribution and transport	Other commercial sectors
I work exclusively in IT security	39%	48%	41%	35%	24%	57%	27%	17%	40%	54%
The majority of my work involves IT security	31%	32%	53%	29%	47%	24%	36%	35%	21%	19%
Some of my work involves IT security but I have other responsibilities	30%	21%	6%	35%	29%	20%	37%	48%	40%	28%