Crypto-Ransomware

Survey of IT Experts

Researchscape International 2/4/16 Jeffrey Henning

EXECUTIVE SUMMARY

Researchscape surveyed 275 IT experts from January 15 to January 30, 2016. These vendors reported that the top security concerns of their customers in 2016 were hacking and privacy breeches (reported by ~65% of respondents). While crypto-ransomware attacks weren't always among the top concerns for customers, a quarter of IT experts (24%) said customers regarded them as a top security concern.

With the new year, 37% of IT vendors said that they were extremely or very concerned about ransomware attacks on their customers. With more than a third of IT vendors concerned about ransomware attacks, the majority of them expect the number of attacks to increase in some degree (59%), with a third expecting a slight increase. Over four out of ten vendors report that customers (43%) have fallen victim to ransomware.

Certain industries are prime targets for those who wish to deal digital harm to them, especially with ransomware attacks. The three industries that had the most affected customers were information technology, accounting/finance/banking, and the internet. Of those effected by the attacks, on average 3 days without access to their data was experience, though the most common answer was only 1 day.

When it came down to it, three quarters of IT experts said that their customer didn't pay the ransom but for those who did the customers paid $250 per user for the ransom (median ransom). Of those who paid, 71% had their files restored. Three quarters of IT vendors said that the customers' computers were wiped and restored in order to remove the virus. Customers spent 3 days or less wiping and restoring all the affected computers, with 13% spending less than 8 hours, though 7% spent more than a week.

Almost half of the IT experts said that they had seen some sort of increase in the volume of support inquiries related to ransomware in the past year. Just under one third of IT experts (27%) said that their customers were very or completely likely to hold their business responsible if they were to fall victim to ransomware.

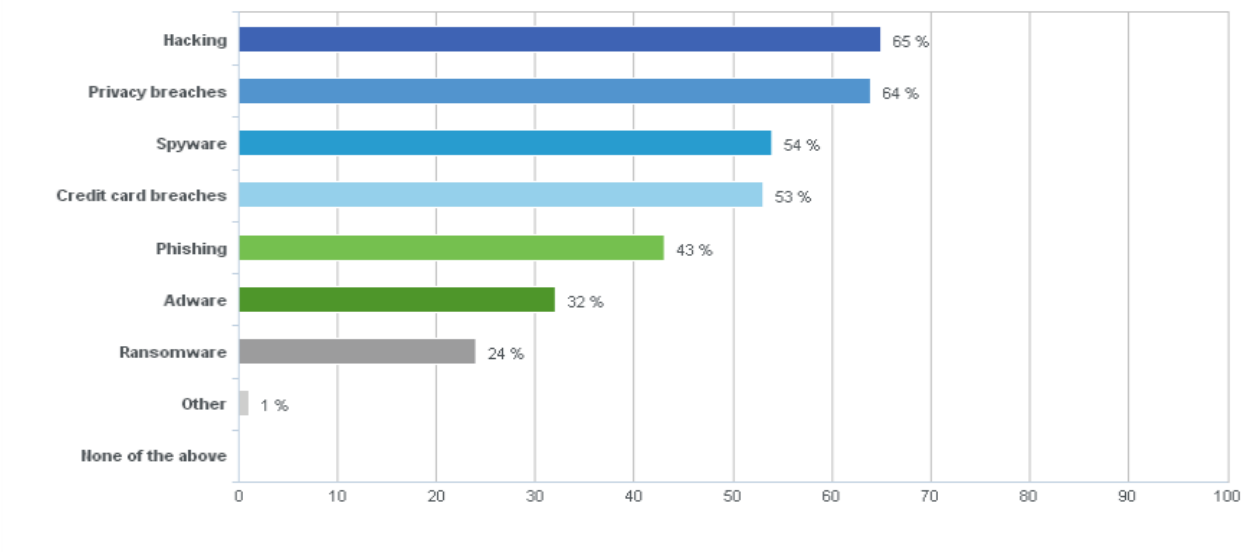
TABLE OF CONTENTS

TABLE OF EXHIBITS

EXTENT OF PROBLEM

Even paranoids have enemies, goes the old saying. Yet with the world always connected and more corporate and personal information stored online than ever before, organizations are rightfully deeply worried about keeping their data safe and secure. To the customers of the IT experts we surveyed, hacking was the top security concern in 2016, followed by privacy breeches (65% and 64% respectively). Ransomware was the top concern of a quarter of organizations (24%).

What are the top security concerns of your customers in 2016? (Select all that apply.)



Sample Size: 275 (All Respondents)

What are the top security concerns of your customers in 2016? (Select all that apply.)

Rank	Option	Response %
1	Hacking	65%
2	Privacy breaches	64%
3	Spyware	54%
4	Credit card breaches	53%
5	Phishing	43%
6	Adware	32%
7	Ransomware	24%
8	Other	1%
9	None of the above	<1%

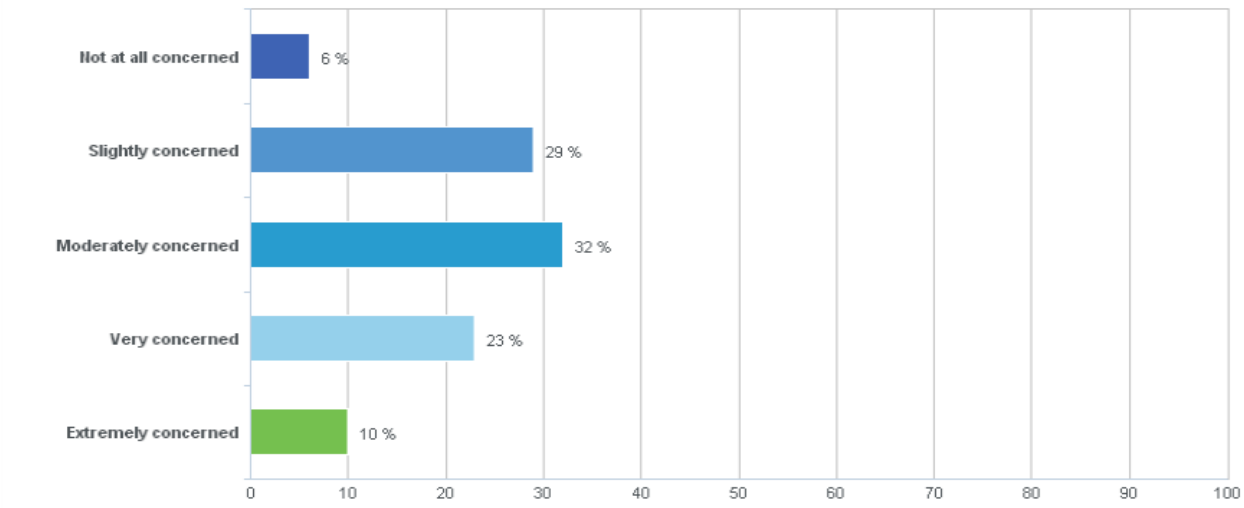
Note: Respondents could select multiple options

Examples of "Other (please specify)" responses: *What are the top security concerns of your customers in 2016? (Select all that apply.)*

- "Loss of data."
- "Chinese Hackers."
- "Malware."

While ransomware attacks weren't the biggest concern of customers, one third of IT experts were very or extremely concerned over them, and nearly as many moderately concerned.

How concerned were you about ransomware attacks on your customers in 2015?



Sample Size: 275 (All Respondents)

With the new year, 37% of IT vendors said that they were extremely or very concerned about ransomware attacks on their customers, up 4 points from 2015.

How concerned were you about ransomware attacks on your customers in 2015? How concerned are you about ransomware attacks on your customers in 2016?

Option	2015	2016
Not at all concerned	6%	5%
Slightly concerned	29%	24%
Moderately concerned	32%	33%
Very concerned	23%	24%
Extremely concerned	10%	13%

Note: Only a single option could be selected

Managed Service Providers are more concerned than others about ransomware attacks this year: 23% of MSPs are extremely concerned, compared to 10% of IT consultants and 0% of VARs.

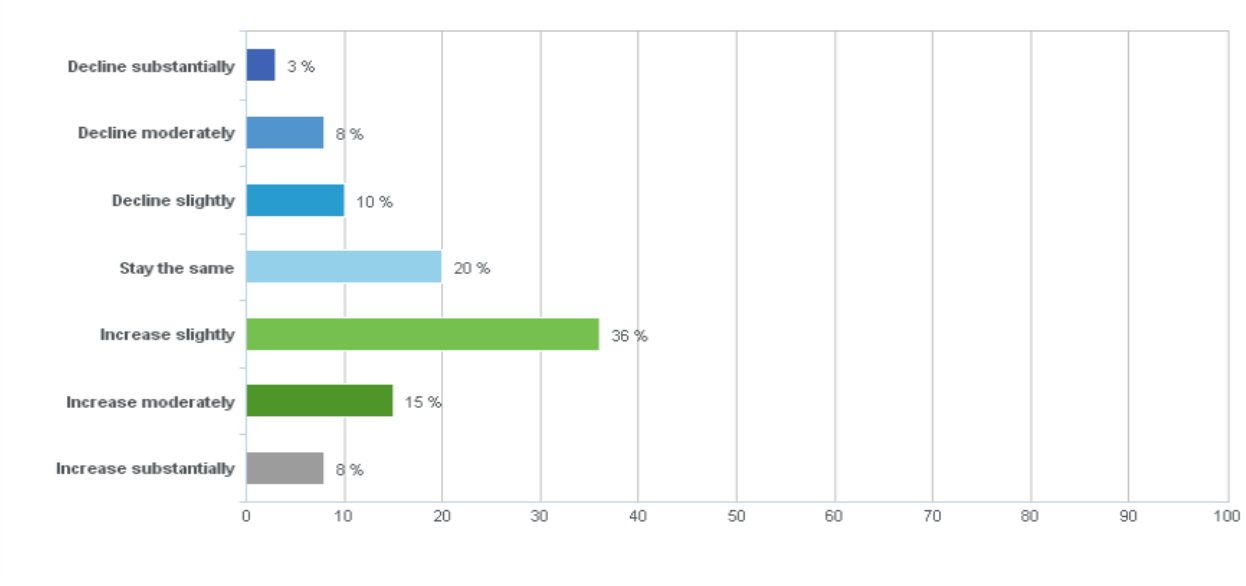
	Which of the following best describes your company?				
	Total	Managed Service Provider	Value-added Reseller	IT Consultant	Other
	(%)	(%)	(%)	(%)	(%)
Total	100	24	5	67	4
Not at all concerned	5	9	7	⇓ 3	17
Slightly concerned	24	20	21	27	8
Moderately concerned	33	29	29	34	42
Very concerned	24	20	43	25	17
Extremely concerned	13	⇑ 23	0	⇓ 10	17

⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

With more than a third of IT experts concerned about ransomware attacks, the majority of them expect the number of ransomware attacks to increase to some degree (59%), with a third expecting a slight increase. Only 3% are optimistic and expect a substantial decline in attacks this year.

How do you expect the number of ransomware attacks to change in 2016?



Sample Size: 275 (All Respondents)

The greater the expectation for an increase in ransomware attacks, the higher the level of concern.

	How concerned are you about ransomware attacks on your customers in 2016?					
	Total	Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
	(%)	(%)	(%)	(%)	(%)	(%)
Total	100	5	24	33	24	13
Decline substantially	3	0	4	1	1	6
Decline moderately	8	20	10	7	4	6
Decline slightly	10	13	15	9	7	6
Stay the same	20	40	⇑ 37	20	⇓ 6	9
Increase slightly	36	20	31	⇑ 49	34	23
Increase moderately	15	0	⇓ 1	11	⇑ 39	14
Increase substantially	8	7	⇓ 0	⇓ 3	7	⇑ 37

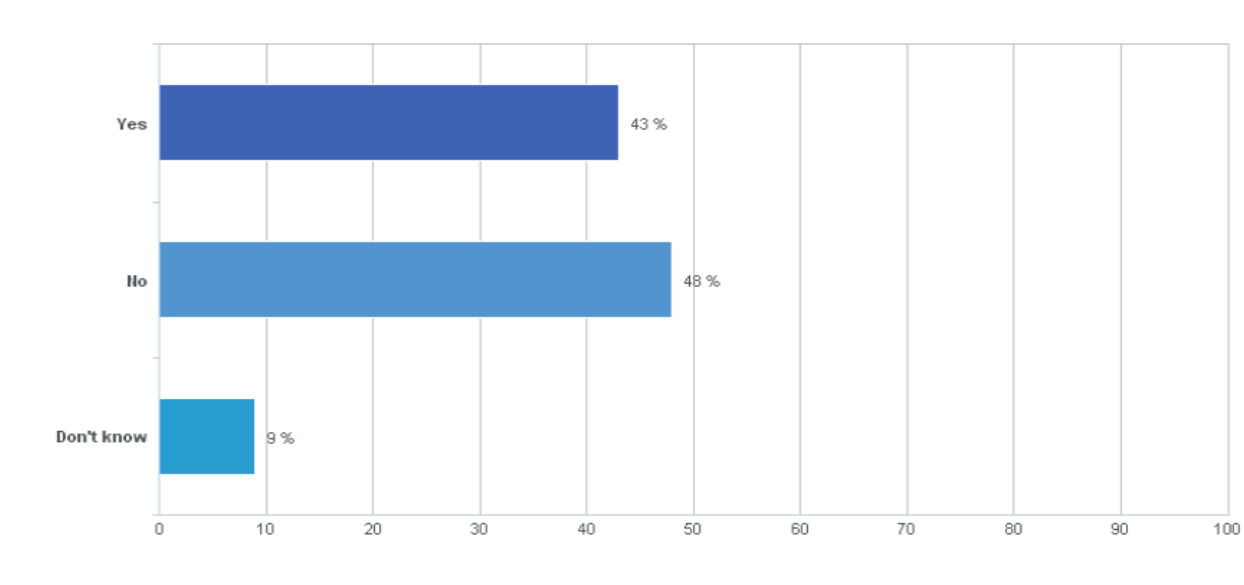
⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

RANSOMWARE ATTACK PROFILE

Over four out of 10 IT experts (43%) have had customers fall victim to ransomware.

Have any of your customers fallen victim to ransomware?



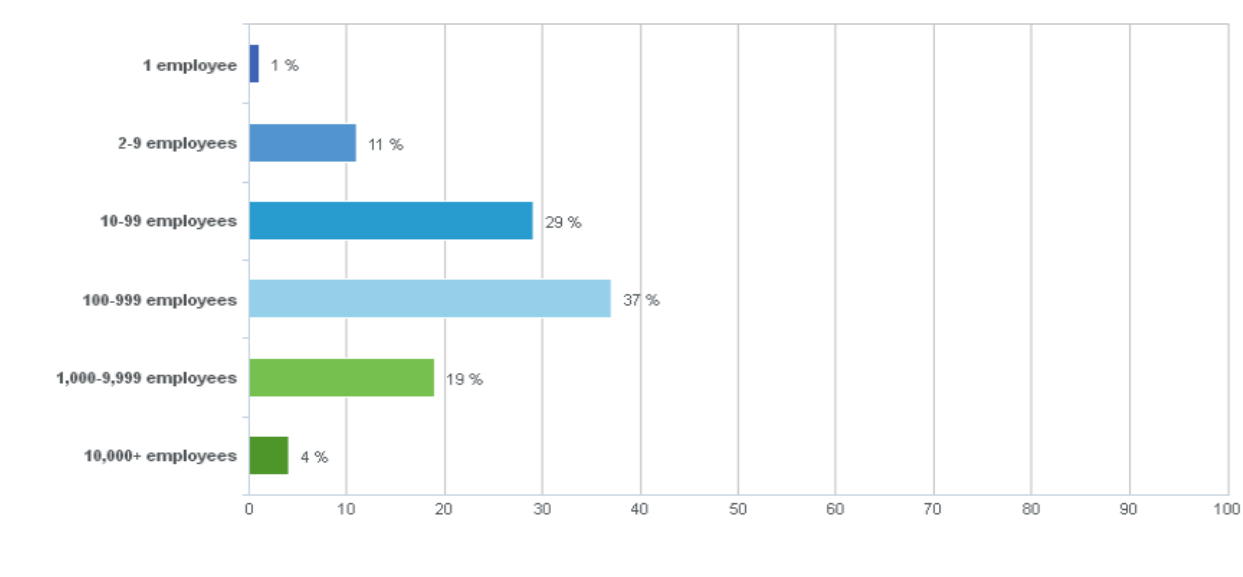
Sample Size: 275 (All Respondents)

We then asked respondents whose firms had dealt with a ransomware attack on a customer to describe in detail the attack that they knew the most about.

Attacks were widespread, and cut across over 22 different industries.

The typical (median) size of an affected customer organization was 100-999 employees (37%). On either end of the extreme, 25% of the ransomware attacks happened to enterprises (1,000+ employees) and 41% happened to small businesses (< 100 employees).

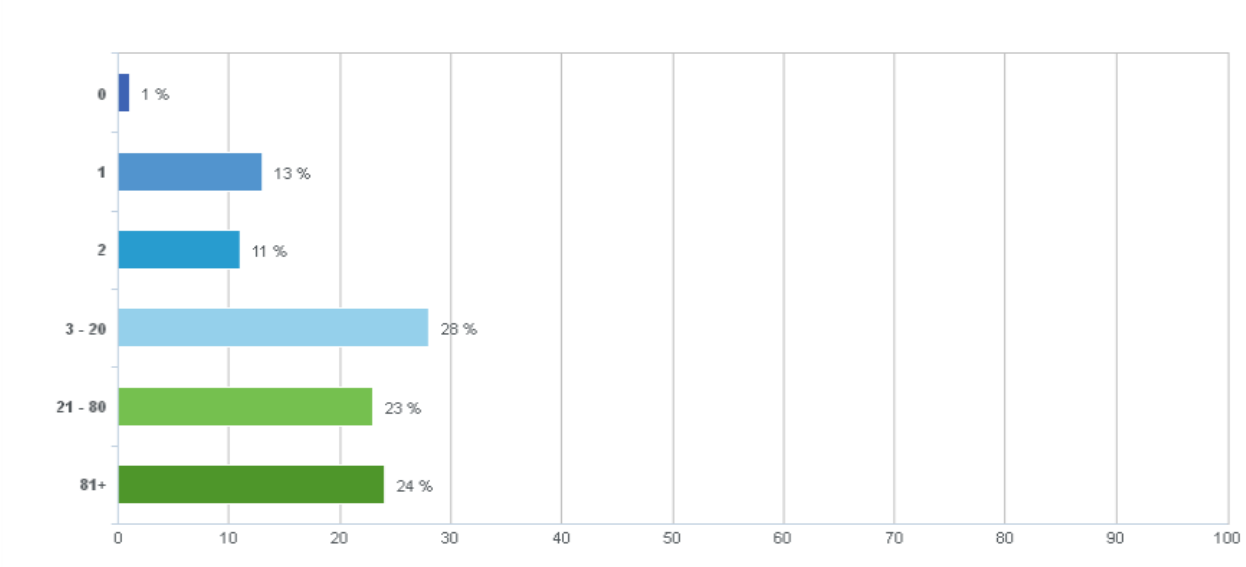
How many employees does this organization have in total?



Sample Size: 114 (41% of Respondents)

The least selected choice was 1 employee (1%). The median number of affected employees was 17, but the most frequent answer was 1 employee (13%) while one organization had 50,000 employees affected.

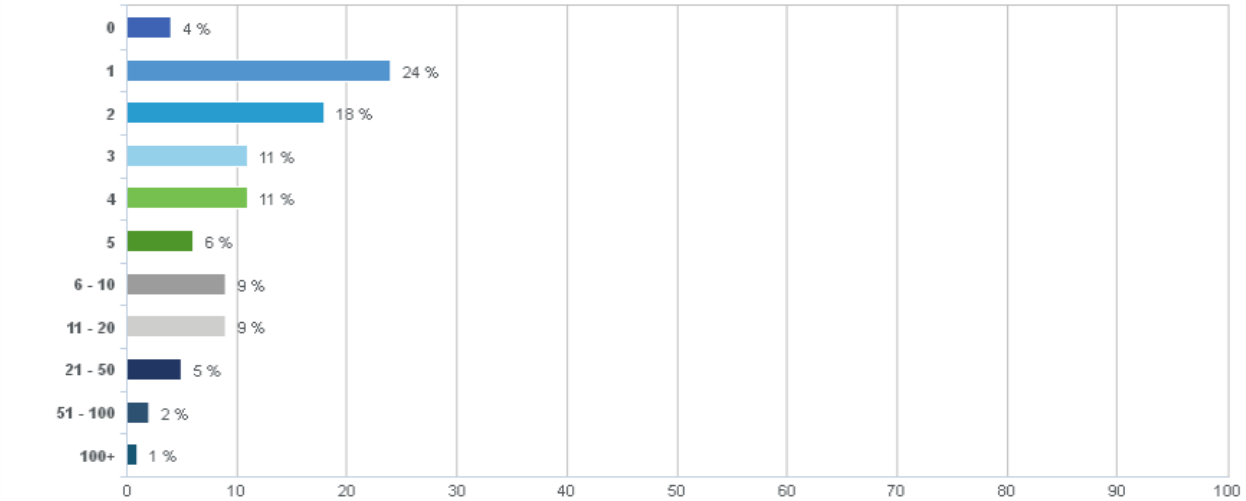
Approximately how many employees in the organization were affected?



Sample Size: 114 (41% of Respondents)

Those affected by the attacks experienced 3 days on average without access to their data, though the most common answer was only 1 day. Some said that there weren't any days lost while one respondent said more than a year of data access was lost.

How many days were employees without access to their data?

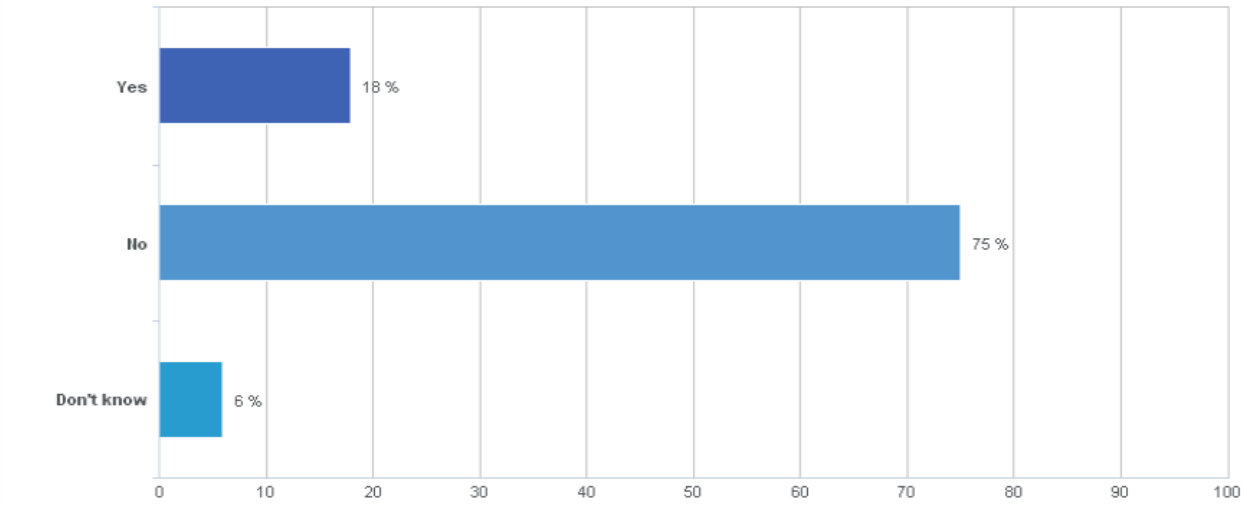


Sample Size: 114 (41% of Respondents)

Ransom Payments

When it came down to it, three quarters of IT vendors (75%) said that the affected customer didn't pay the ransom.

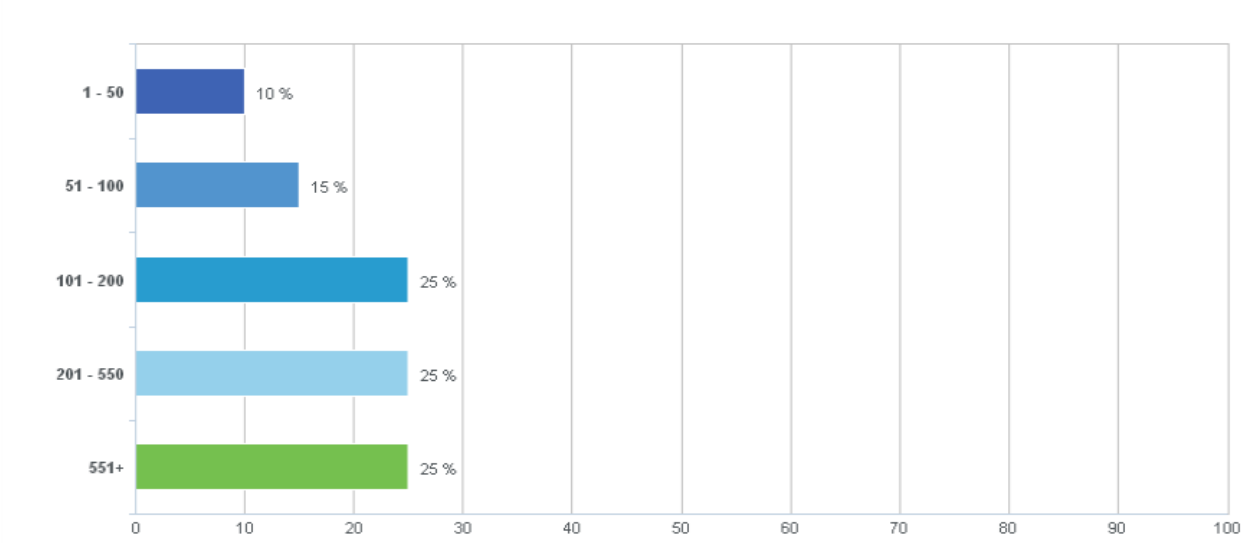
Did your client pay the ransom?



Sample Size: 114 (41% of Respondents)

The median amount that customers paid was $250 per user for the ransom, with the most common amount paid being $100 per user. One fourth of the ransoms were $551 or higher.

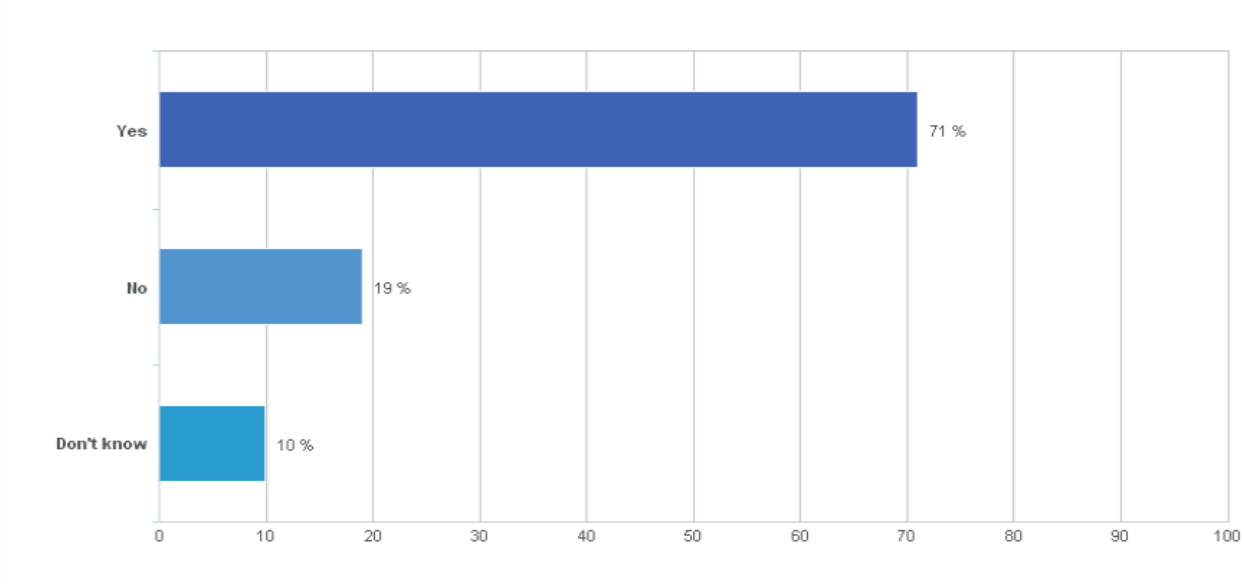
What was the amount paid per user?



Sample Size: 20 (7% of Respondents)

While 71% of ransomware pirates restored the customers' files after being paid off, 1 in 5 customers who paid the ransom, failed to recover their files.

Did the ransomware restore their files after payment was confirmed?

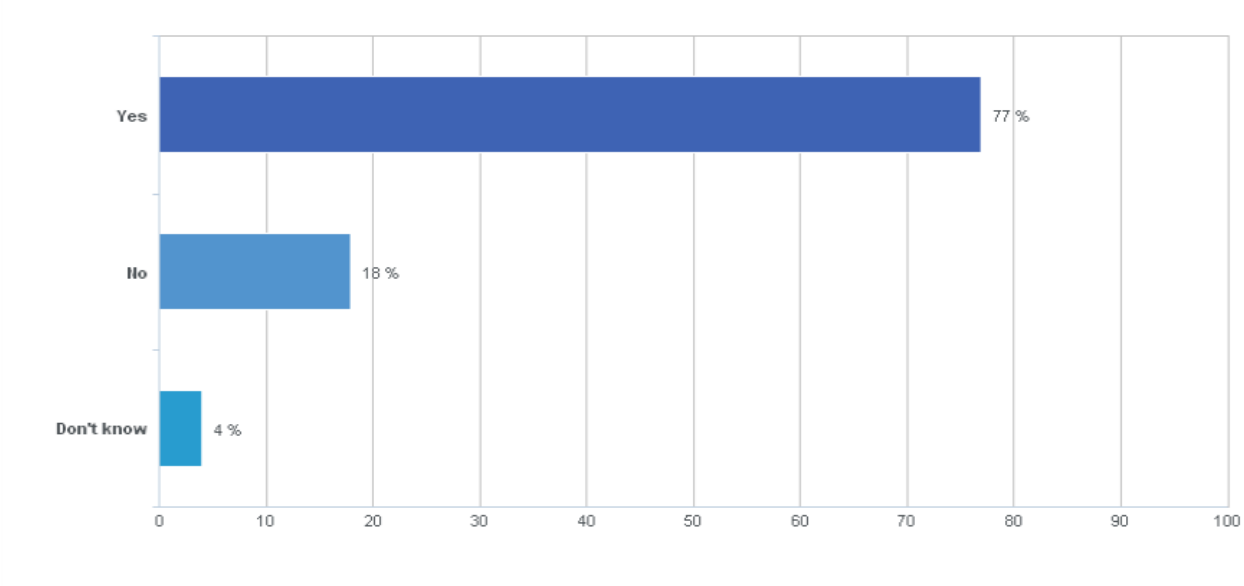


Sample Size: 21 (8% of Respondents)

Removing the Virus

Three quarters of IT vendors said that the customers' computers were wiped and restored in order to remove the virus, though 18% didn't.

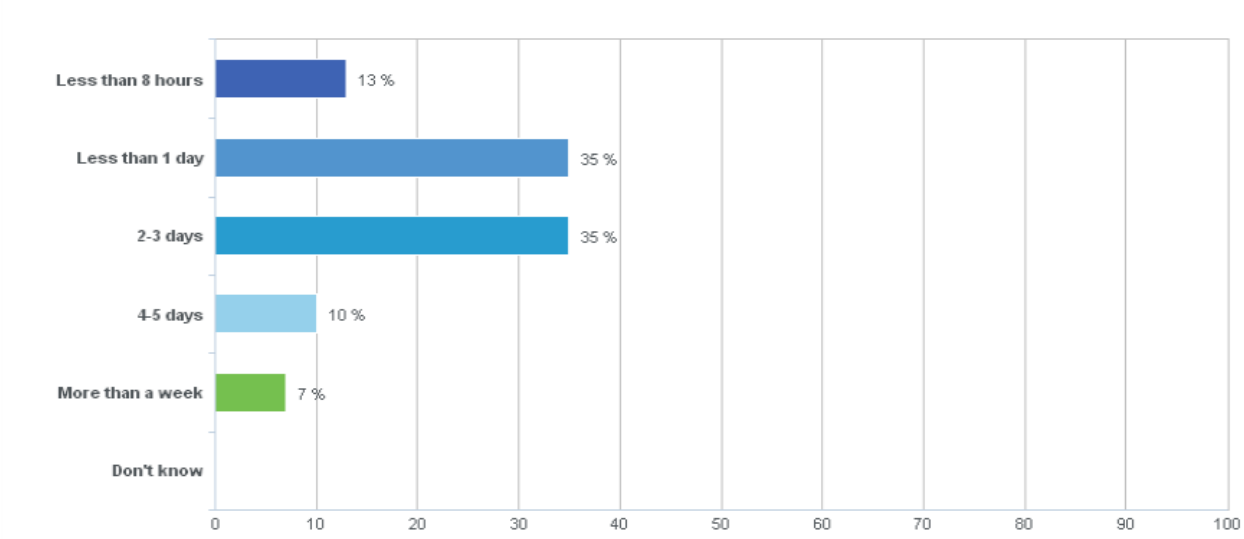
Were your customers' computers wiped and restored to remove the virus?



Sample Size: 114 (41% of Respondents)

The majority of the consultants spent 3 days or less wiping and restoring all the affected computers, with 13% spending less than 8 hours, though 7% spent more than a week.

How much elapsed time did it take to complete the entire wipe and restore process for all affected computers?



Sample Size: 88 (32% of Respondents)

Using rough estimates, MSPs were the fastest, completing the entire wipe and restore process in 45 hours, while IT consultants took 53 hours, and VARs took 72.

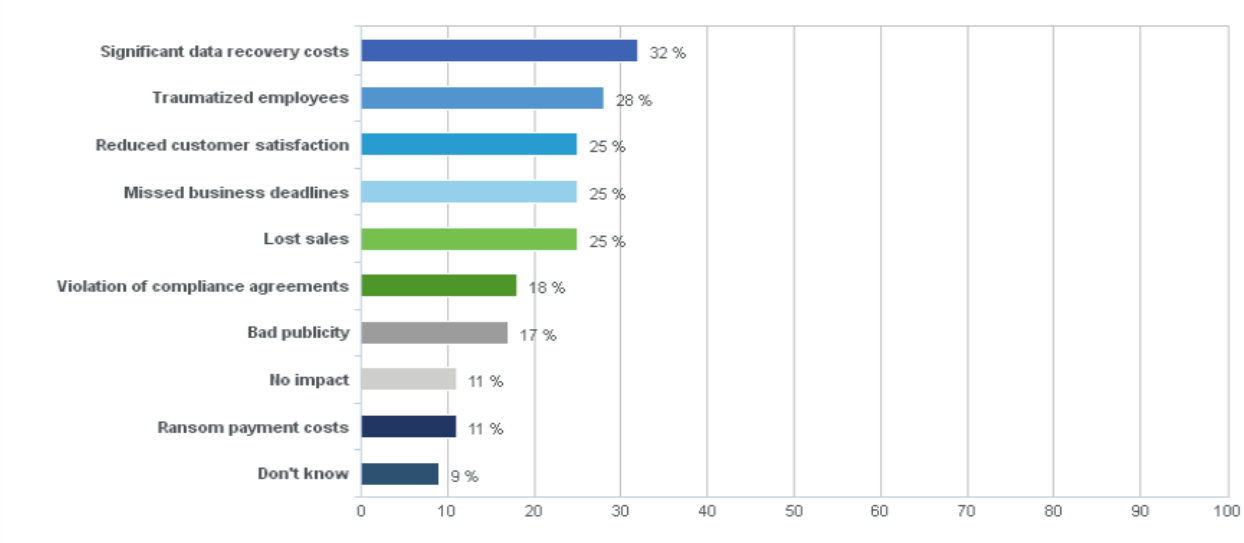
	Which of the following best describes your company?				
	Total	Managed Service Provider	Value-added Reseller	IT Consultant	Other
	(%)	(%)	(%)	(%)	(%)
Total	100	27	5	64	5
Less than 8 hours	13	25	0	9	0
Less than 1 day	35	25	25	39	50
2-3 days	35	42	50	30	50
4-5 days	10	0	0	⇑ 16	0
More than a week	7	8	25	5	0
Don't know	0	0	0	0	0
[Estimated hours]	51	45	72	53	42

⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

The ransom payment cost had a business impact of only 11%, the lowest business impact. Significant data recovery costs were the top business impact caused by the ransomware outbreak (32%), followed by traumatized employees (28%). Grouped together, and mentioned 25% of respondents each, were reduced customer satisfaction, missed business deadlines, and lost sales.

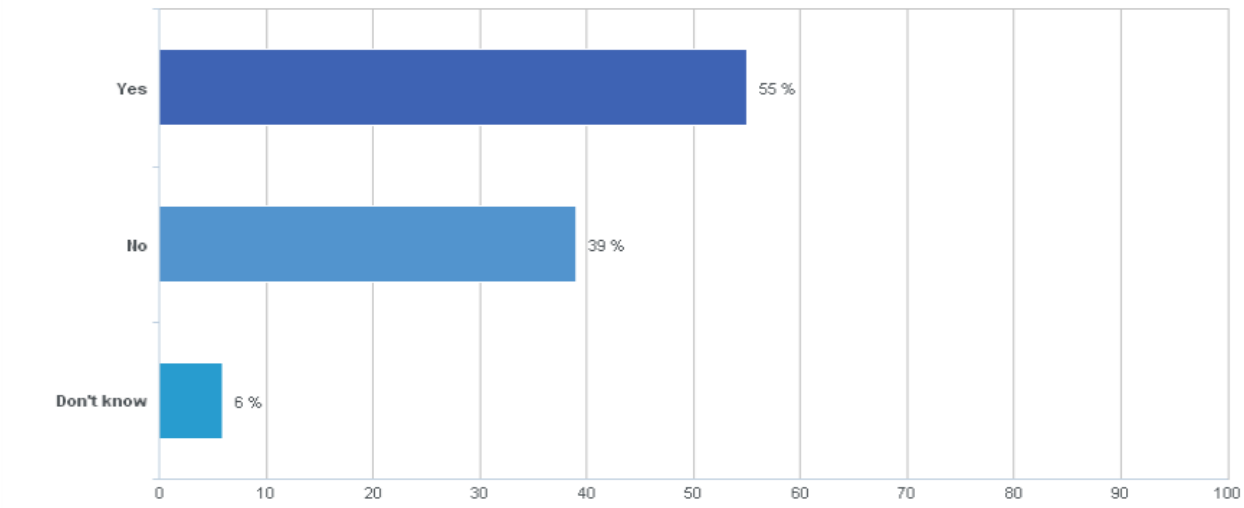
What was the business impact, if any, of the ransomware outbreak? (Select all that apply.)



Sample Size: 114 (41% of Respondents)

While the majority (55%) of IT experts billed their customers for the time spent helping them recover their data, a large percentage (39%) reported they did not bill for the time spent on recover.

Did you bill your customers additionally for the time spent helping them recover?

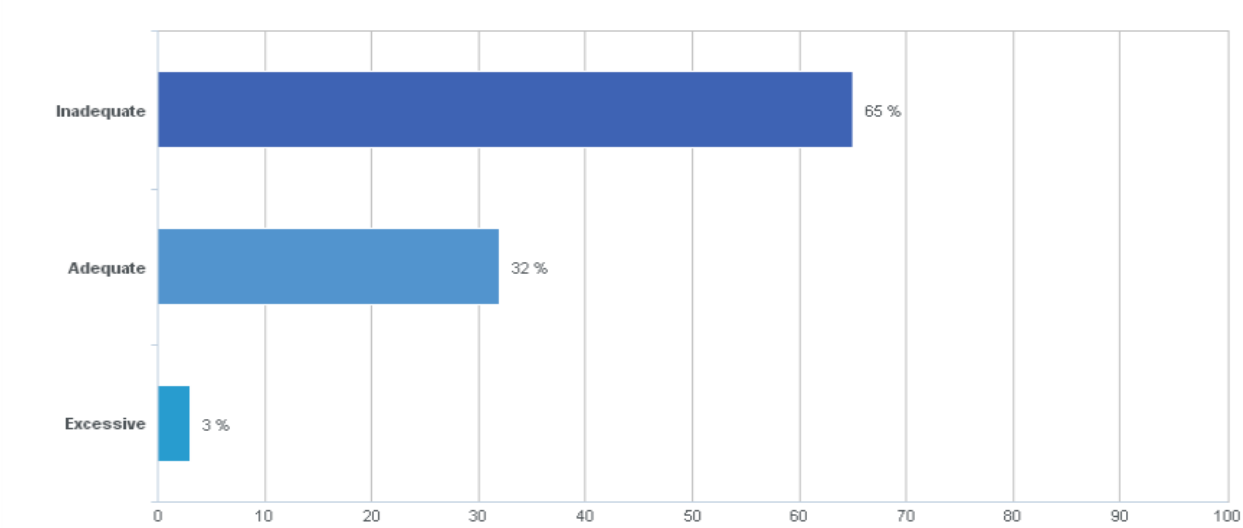


Sample Size: 114 (41% of Respondents)

MSP/VAR ATTITUDES TOWARDS RANSOMWARE

65% of IT experts believe that law enforcement's efforts to combat ransomware are inadequate. At the other extreme, 3% said it was excessive.

How would you describe law enforcement's efforts in combatting ransomware?



Sample Size: 259 (94% of Respondents)

19 out of 20 IT vendors (94%) who were extremely concerned about ransomware knew how to protect their customers, compared to 80% of everyone else.

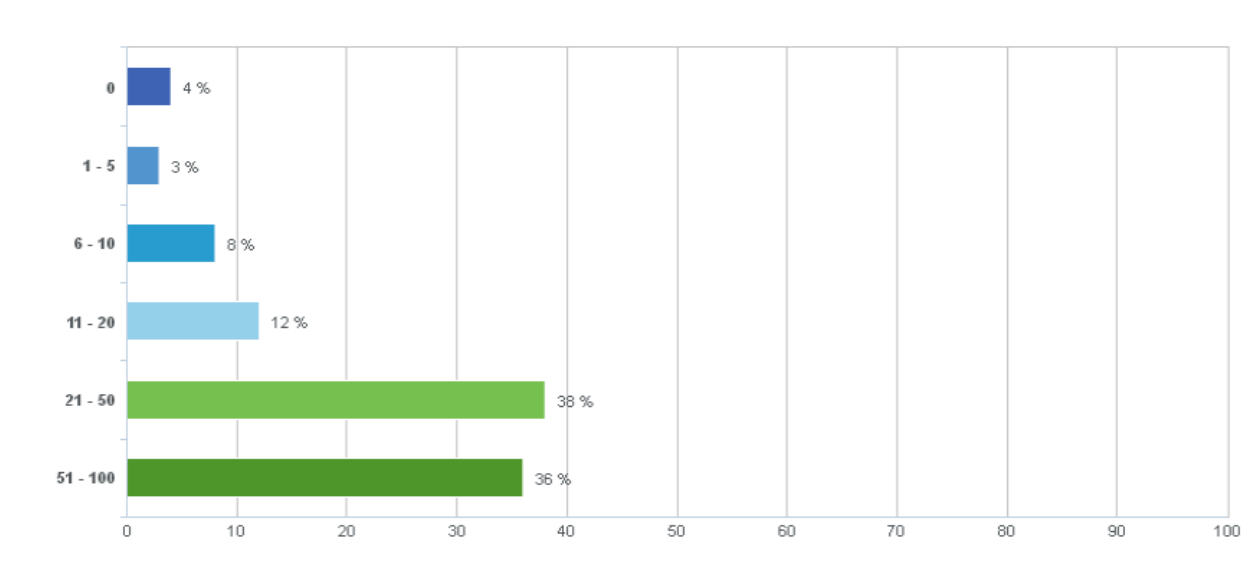
How concerned are you about ransomware attacks on your customers in 2016?						
	Total	Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
	(%)	(%)	(%)	(%)	(%)	(%)
Total	100	5	24	32	26	13
Yes	81	54	85	80	79	⇑ 94
No	19	46	15	20	21	⇓ 6

⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

IT experts reported that about half of their customers were willing to pay an incremental fee for a ransomware business continuity solution.

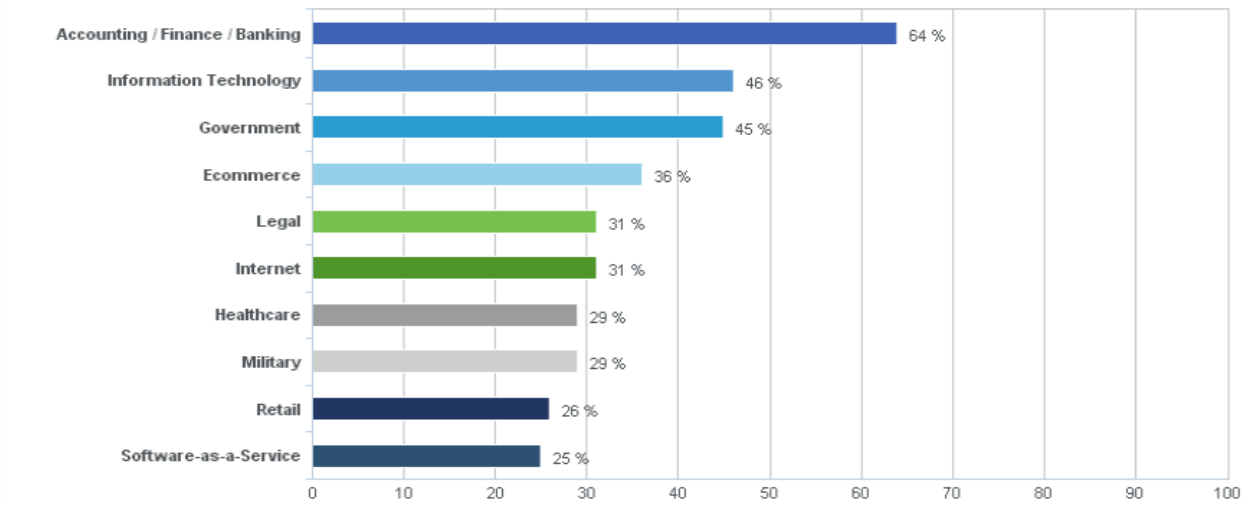
What percent of your customers would be willing to pay an incremental fee for a ransomware business continuity solution?



Sample Size: 256 (93% of Respondents)

According to the IT experts surveyed, the industry that would stand to lose the most from ransomware was accounting/finance/banking (64%), followed by information technology (46%), and then government (45%).

What industries stand to lose the most from ransomware? (Select all that apply.)



Sample Size: 259 (94% of Respondents)

What industries stand to lose the most from ransomware? (Select all that apply.)

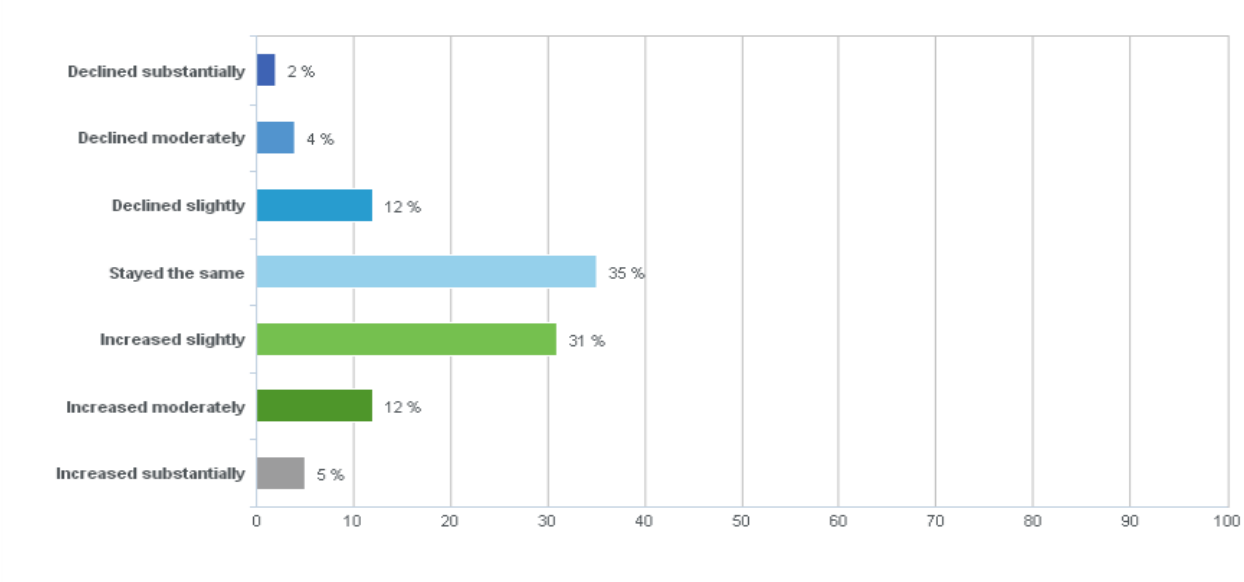
Option	Response %	Option	Response %
Accounting / Finance / Banking	64%	**Manufacturing**	11%
Advertising / Graphic Design	13%	**Military**	29%
Arts & Entertainment	11%	**Non-profit**	7%
Clerical	9%	**Professional Services**	23%
Construction	5%	**Public Safety**	17%
Ecommerce	36%	**Publishing**	7%
Education	12%	**Real Estate**	16%
Government	45%	**Retail**	26%
Healthcare	29%	**Software-as-a-Service**	25%
Information Technology	46%	**Travel & Hospitality**	15%
Internet	31%	**Transportation**	15%
Legal	31%	**Wholesale**	9%
		Other	<1%

Note: Respondents could select multiple options

CUSTOMER ATTITUDES TOWARDS RANSOMWARE

Almost half of the IT experts said that they had seen an increase in the volume of support inquiries over the past year (48%). Only 18% saw a decline.

How has the volume of support inquiries related to ransomware changed in the past year?



Sample Size: 256 (93% of Respondents)

Those who had seen an increase had grown more concerned about the threat of ransomware as a result.

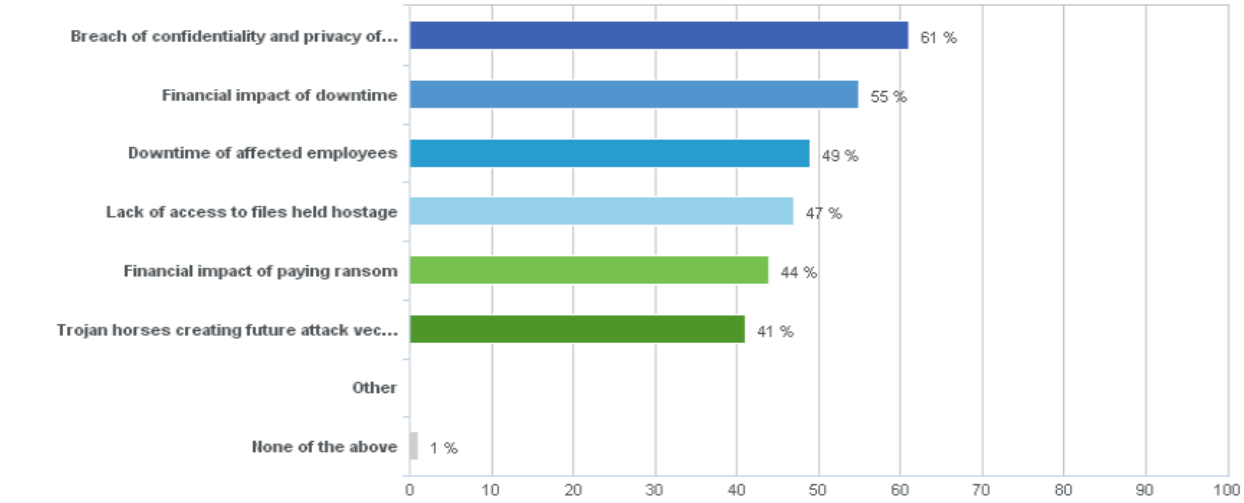
	How concerned are you about ransomware attacks on your customers in 2016?					
	Total	Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
	(%)	(%)	(%)	(%)	(%)	(%)
Total	100	5	24	32	26	13
Declined substantially	2	8	2	0	2	3
Declined moderately	4	15	6	1	5	3
Declined slightly	12	8	16	11	9	12
Stayed the same	35	46	⇑ **56**	38	⇓ 21	⇓ 9
Increased slightly	31	15	⇓ 18	⇑ **44**	32	30
Increased moderately	12	0	⇓ 2	⇓ 5	⇑ **29**	18
Increased substantially	5	8	⇓ 0	1	3	⇑ **24**

⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

Respondents' concerns about ransomware's impact on their customers focused mainly on breach of confidentiality and privacy of affected files (61%), followed by the financial impact of downtime (55%), and downtime of affected employees (49%). Other concerns included being able to get back up after the attack.

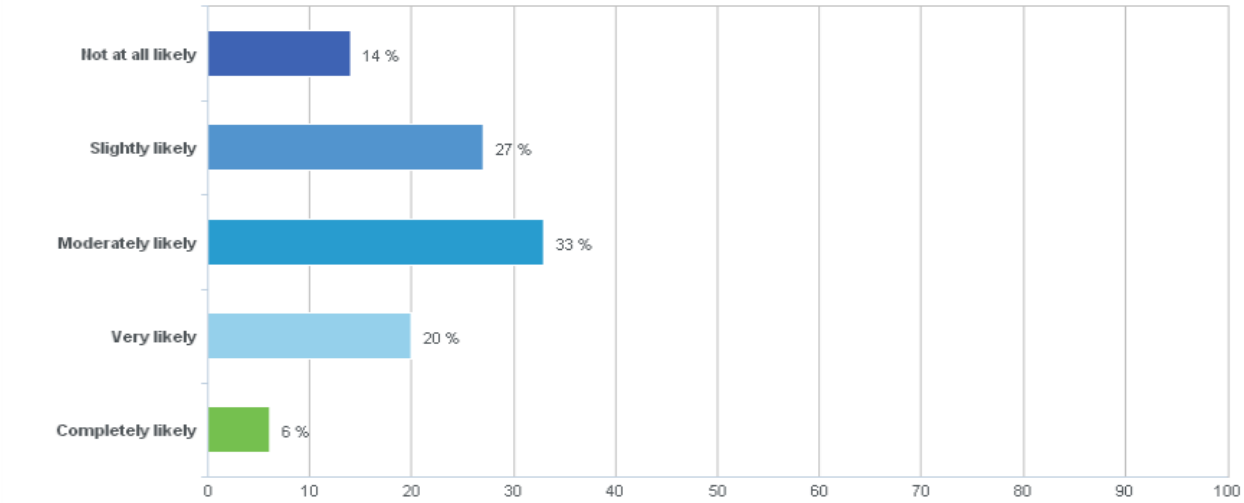
What are your concerns about ransomware's impact on your customers?



Sample Size: 256 (93% of Respondents)

Just under one third of IT experts (27%) said their customers were very or completely likely to hold their business responsible if they were to fall victim to ransomware.

How likely are your customers to hold your business responsible if they were to fall victim to ransomware?



Sample Size: 256 (93% of Respondents)

The more concerned about ransomware that they were, the more likely that they believed their customers would hold them responsible. Of those who were extremely concerned, 27% reported their customers would be completely likely to hold them responsible vs. 3% of everyone else.

How concerned are you about ransomware attacks on your customers in 2016?						
	Total	Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
	(%)	(%)	(%)	(%)	(%)	(%)
Total	100	5	24	32	26	13
Not at all likely	14	31	19	10	11	12
Slightly likely	27	23	34	28	24	18
Moderately likely	33	31	31	⇑ **41**	29	24
Very likely	20	8	13	18	⇑ **33**	18
Completely likely	6	8	3	2	3	⇑ **27**

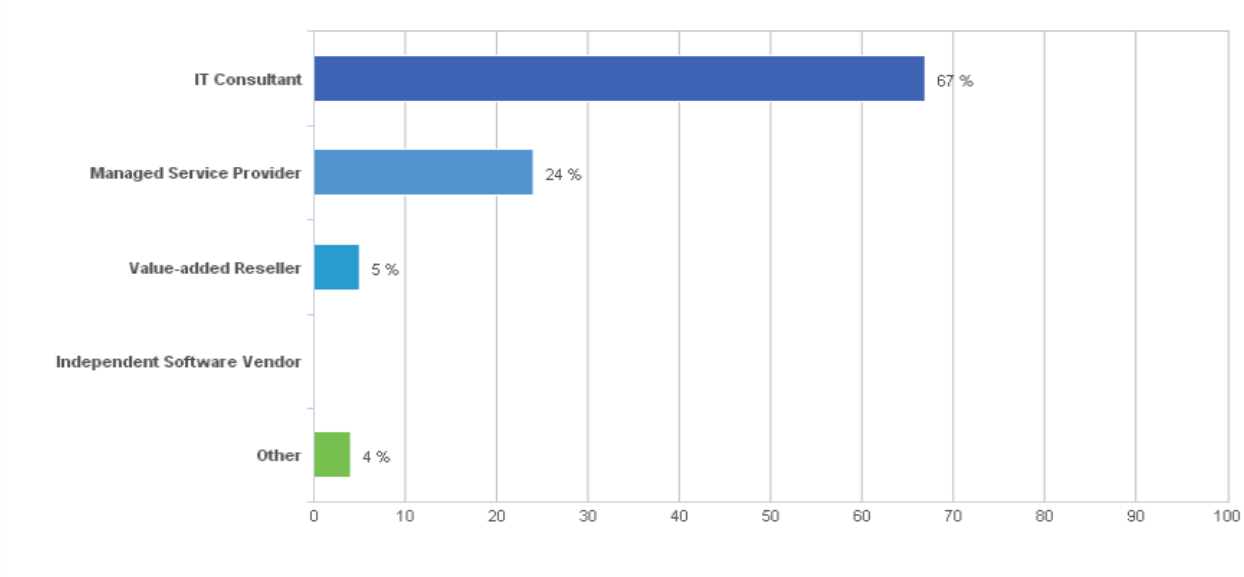
⇑ *indicates cells that are significantly greater than all other cells in this row at a 95% confidence level.*

⇓ *indicates cells that are significantly less than all other cells in this row at a 95% confidence level.*

FIRMOGRAPHICS

More than half of the IT experts came from companies that would best be described as IT Consultants (67%), followed by Managed Service Providers (24%).

Which of the following best describes your company?



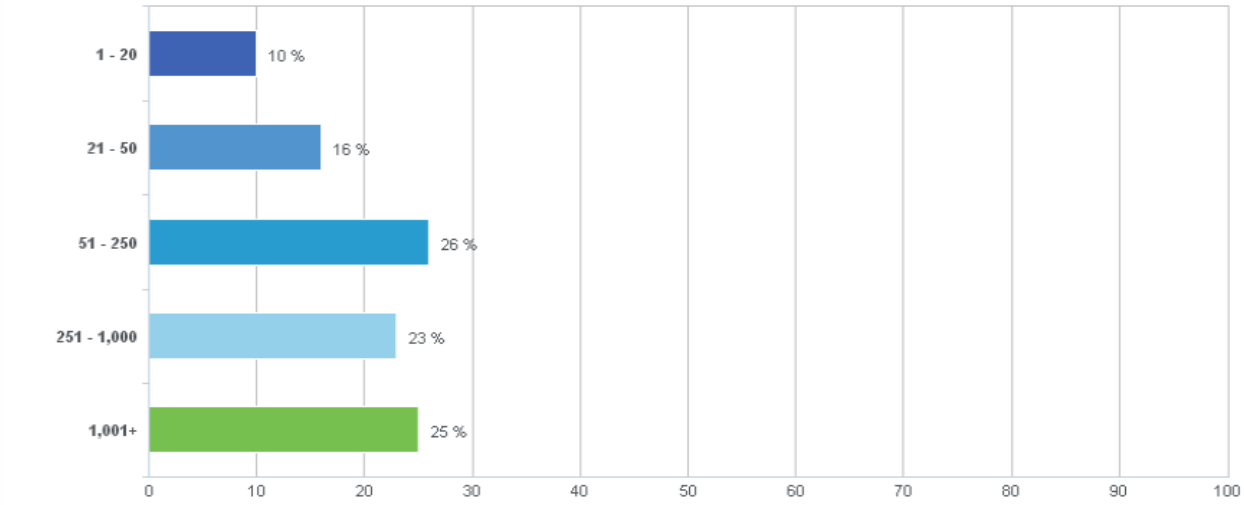
Sample Size: 275 (All Respondents)

Representative "Other (please specify)" responses to: *Which of the following best describes your company?*

- "Hardware reseller."
- "Hardware and software."
- "Communication/IT."
- "Provides service for companies."
- "Service broken down ATMs."

On average, IT experts had 250 customers, with most having about 50 customers with outlying answers of as low as 2 and as high as 10,000,000.

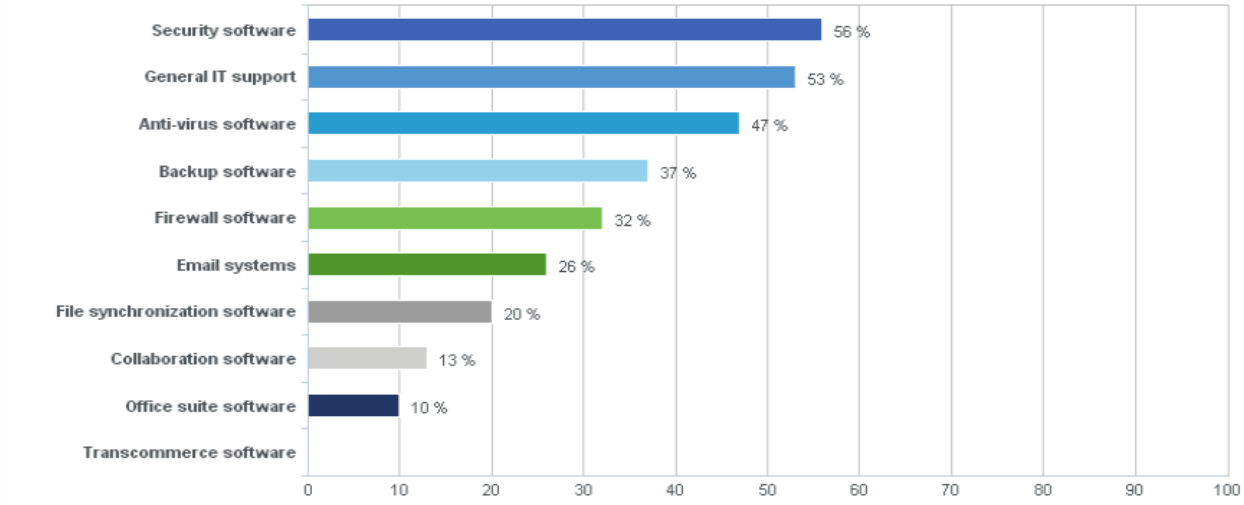
Approximately how many customers does your organization have?



Sample Size: 254 (92% of Respondents)

Security software (56%), general IT support (53%), and anti-virus software (47%) were the three most selected solutions that the IT vendors' companies sell.

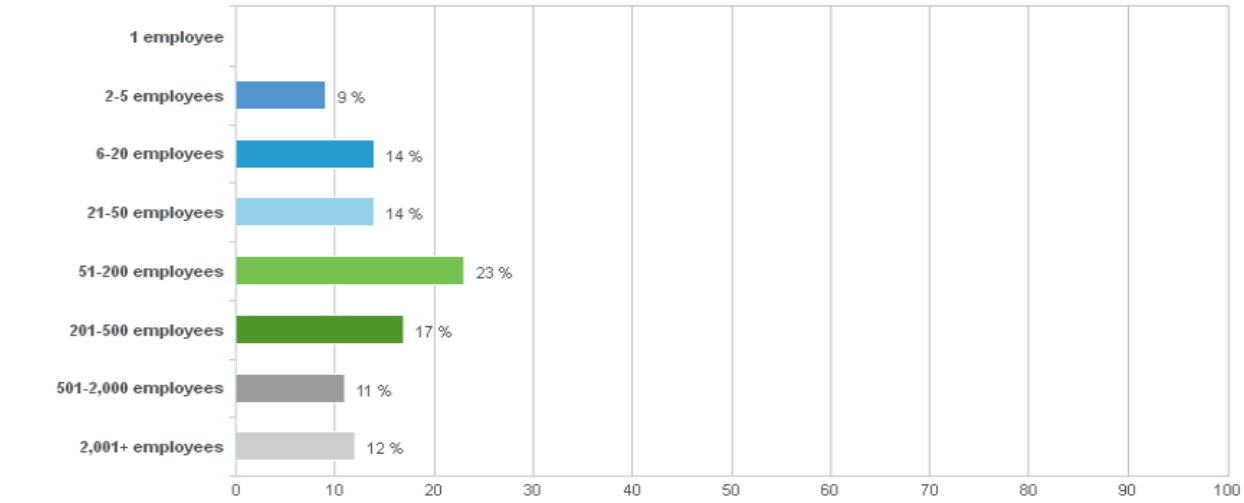
Which of the following solutions does your company sell? (Select all that apply.)



Sample Size: 275 (All Respondents)

The most typical respondent came from companies that employed 51-200 employees (23%), representing the median and the mode. Another 40% of respondents came from larger firms.

How many employees work for your company?



Sample Size: 275 (All Respondents)

Top quotes for: *(Optional) We appreciate your time and welcome your feedback on any aspect of this topic or questionnaire.*

- "I was actually surprised and impressed that it was about ransomware. It really is one of the most severe problems that many of our clients have had over the past few years. A failed hard drive can be very frustrating and a possible loss for all data, and ransomware has made some of our customer's data unrecoverable. And, it was done intentionally and maliciously by some individuals, which seems to make the matter feel a bit worse since it was something that did not need to happen. It would be nice if something could be done to the individuals who caused this."
- "It appears the medical industry is vulnerable and could be difficult to control due to various 3rd party vendors."
- "A lot of resistance to solutions comes from an ongoing cost on a monthly basis versus a onetime cost for prevention or fix afterwards, even though it might be more expensive."
- "File-sharing services have become near-ubiquitous among enterprise users. ... a thought-out roadmap of how the present FSS solution can be upgraded to the ... collaboration, and synchronization and backups from Windows, Linux, Mac, iOS ..."

- "Thanks for a survey that is about my field of work. I haven't been able to find many of these."
- "Common Issue: Adware that start tracking browsing habits, redirecting search sessions to unwanted sites without permission, and causing other unfair activities."
- "From my experiences with everything, the problem has always been insiders, and on rare occasions someone has used social engineering to gain access and stolen a whole server."

APPENDIX A - RESEARCHSCAPE METHODOLOGY

Researchscape surveyed 275 IT experts using an online survey fielded from January 15 to January 30, 2016. The survey results were not weighted.

Respondents were recruited from a number of third-party panels. Each respondent had their identity validated and only one response was permitted per respondent, even if they were members of multiple panels. Each respondent was offered points towards rewards in exchange for their participation.

As this was not a probability-based sample, calculating the theoretical margin of sampling error is not applicable. However, as with probability surveys, it is important to keep in mind that results are estimates and typically vary within a narrow range around the actual value that would be calculated by completing a census of everyone in a population. Again, as with probability surveys, on occasion the results from a particular question will be completely outside a typical interval of error.

We included the responses from incomplete surveys; 39 respondents did not complete the entire questionnaire. A common reason that respondents abandon surveys is because of topic salience: they simply find the subject of a survey to be uninteresting to them. Including their answers for those questions to which they did respond improves the representativeness of results, which would otherwise skew towards those with a higher engagement with the topic of the study.

There are many types of survey errors that can limit the ability to generalize to a population. Throughout the research process, Researchscape followed a Total Survey Quality approach designed to minimize error at each stage. Total Survey Quality, also known as Total Survey Error, recognizes that multiple sources of error can reduce the validity of survey research. Besides sampling error, five types of non-sampling error can occur: specification error, frame error, nonresponse error, measurement error, and processing error. At each step in the survey research process, the research team followed best practices and used quality controls to minimize the impact of these sources of error. Researchscape is confident that the information gathered from this survey can be used to make important business decisions related to this topic.

We only report differences between subgroups when they are statistically significant at the 95% confidence level. While this is the industry standard for reporting results, it does mean that reported differences are simply due to chance 1 out of 20 times. Differences were only reported if they were statistically significant and were deemed to have some practical significance. All closed-ended questions in the survey were cross-tabulated by:

- Which of the following best describes your company?
- Which of the following solutions does your company sell? (Select all that apply.)
- How many employees work for your company?

- What are the top security concerns of your customers in 2016? (Select all that apply.)
- How concerned are you about ransomware attacks on your customers in 2016?

Researchscape International is a market-research consultancy providing "Do It for You" surveys at Do It Yourself prices. For questions about this or other research, please contact us at +1-888-983-1675 x 1 or visit our website, http://www.researchscape.com/

APPENDIX B - QUESTIONS

Which of the following best describes your company?

Managed Service Provider	24%	
Value-added Reseller	5%	
IT Consultant	67%	
Independent Software Vendor	0%	[TERMINATE]
Other	4%	

Which of the following solutions does your company sell? (Select all that apply.)

Anti-virus software	47%	
Backup software	37%	
Collaboration software	13%	
Email systems	26%	
File synchronization software	20%	
Firewall software	32%	
General IT support	53%	
Office suite software	10%	
Security software	56%	
Transcommerce software	0%	[TERMINATE]
None of the above	0%	[TERMINATE]

How many employees work for your company?

1 employee	0%	[TERMINATE]
2-5 employees	9%	
6-20 employees	14%	
21-50 employees	14%	
51-200 employees	23%	
201-500 employees	17%	
501-2,000 employees	11%	
2,001+ employees	12%	

What are the top security concerns of your customers in 2016? (Select all that apply.)

Adware	32%
Credit card breaches	53%
Hacking	65%
Phishing	43%
Privacy breaches	64%
Ransomware	24%
Spyware	54%
Other	1%
None of the above	<1%

How concerned were you about ransomware attacks on your customers in 2015?

Not at all concerned	6%
Slightly concerned	29%
Moderately concerned	32%
Very concerned	23%
Extremely concerned	10%

How concerned are you about ransomware attacks on your customers in 2016?

Not at all concerned	5%
Slightly concerned	24%
Moderately concerned	33%
Very concerned	24%
Extremely concerned	13%

How do you expect the number of ransomware attacks to change in 2016?

Decline substantially	3%
Decline moderately	8%
Decline slightly	10%
Stay the same	20%
Increase slightly	36%
Increase moderately	15%
Increase substantially	8%

Have any of your customers fallen victim to ransomware?

Yes	43%
No	48%
Don't know	9%

[IF SO] Thinking of these ransomware attacks on your customers, please describe the nature of the attack that you know the most about.

What industry was the affected customer in?

Accounting / Finance / Banking	15%
Advertising / Graphic Design	1%
Arts & Entertainment	2%
Clerical	1%
Construction	3%
Ecommerce	2%
Education	6%
Government	5%
Healthcare	4%
Information Technology	16%
Internet	8%
Legal	4%
Manufacturing	4%
Military	2%
Non-profit	4%
Professional Services	4%
Public Safety	0%
Publishing	1%
Real Estate	2%
Retail	6%
Software-as-a-Service	7%
Travel & Hospitality	2%
Transportation	0%
Wholesale	0%
Other	4%

How many employees does this organization have in total?

1 employee	1%
2-9 employees	11%
10-99 employees	29%
100-999 employees	37%
1,000-9,999 employees	19%
10,000+ employees	4%

Approximately how many employees in the organization were affected?

[OPEN-ENDED]

How many days were employees without access to their data?

[OPEN-ENDED]

Did your client pay the ransom?

Yes	18%
No	75%
Don't know	6%

What was the amount paid per user?

[OPEN-ENDED]

Did the ransomware restore their files after payment was confirmed?

Yes	71%
No	19%
Don't know	10%

Were your customers' computers wiped and restored to remove the virus?

Yes	77%
No	18%
Don't know	4%

How much elapsed time did it take to complete the entire wipe and restore process for all affected computers?

Less than 8 hours	13%
Less than 1 day	35%
2-3 days	35%
4-5 days	10%
More than a week	7%
Don't know	0%

What was the business impact, if any, of the ransomware outbreak? (Select all that apply.)

No impact	11%
Missed business deadlines	25%
Reduced customer satisfaction	25%
Lost sales	25%
Bad publicity	17%
Violation of compliance agreements	18%
Traumatized employees	28%
Significant data recovery costs	32%
Ransom payment costs	11%
Other	0%
Don't know	9%

Did you bill your customers additionally for the time spent helping them recover?

Yes	55%
No	39%
Don't know	6%

How would you describe law enforcement's efforts in combatting ransomware?

Inadequate	65%
Adequate	32%
Excessive	3%

Do you know how to protect your customers from ransomware?

Yes	81%
No	19%

Do you know how to contain a ransomware outbreak?

Yes	73%
No	27%

Approximately how many customers does your organization have?

[OPEN-ENDED]

Approximately what percent of your customers have a business continuity solution for ransomware? (With a business continuity solution for ransomware, IT would roll back to uninfected versions of files without paying the ransom, and users could access those files using alternate devices while IT restores the original device.)

[OPEN-ENDED]

What percent of your customers would be willing to pay an incremental fee for a ransomware business continuity solution?

[OPEN-ENDED]

What industries stand to lose the most from ransomware? (Select all that apply.)

Accounting / Finance / Banking	64%
Advertising / Graphic Design	13%
Arts & Entertainment	11%
Clerical	9%
Construction	5%
Ecommerce	36%
Education	12%
Government	45%
Healthcare	29%
Information Technology	46%
Internet	31%
Legal	31%
Manufacturing	11%
Military	29%
Non-profit	7%
Professional Services	23%
Public Safety	17%
Publishing	7%
Real Estate	16%
Retail	26%
Software-as-a-Service	25%
Travel & Hospitality	15%
Transportation	15%
Wholesale	9%
Other	<1%

How has the volume of support inquiries related to ransomware changed in the past year?

Declined substantially	2%
Declined moderately	4%
Declined slightly	12%
Stayed the same	35%
Increased slightly	31%
Increased moderately	12%
Increased substantially	5%

What are your concerns about ransomware's impact on your customers?

Breach of confidentiality and privacy of affected files	61%
Downtime of affected employees	49%
Financial impact of downtime	55%
Financial impact of paying ransom	44%
Lack of access to files held hostage	47%
Trojan horses creating future attack vectors	41%
Other	<1%
None of the above	1%

How likely are your customers to hold your business responsible if they were to fall victim to ransomware?

Not at all likely	14%
Slightly likely	27%
Moderately likely	33%
Very likely	20%
Completely likely	6%

(Optional) We appreciate your time and welcome your feedback on any aspect of this topic or questionnaire.

[OPEN ENDED]