The Cost & Consequences of Ransomware

for Small to Large-Sized Enterprises

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

Ponemon
INSTITUTE

This is the second study Ponemon Institute has conducted on the devastating impact ransomware attacks have on small to large-sized enterprises. The first study was completed in 2017[1], and as revealed in this research, little progress has been made in mitigating the consequences of these threats.

[1] The Rise of Ransomware, conducted by Ponemon Institute and sponsored by Carbonite. Published in January 2017.

INTRODUCTION

In this year's research

the percentage of companies experiencing an attack increased from 51 percent in the 2017 study to 80 percent. Yet, as shown in Figure 1, 57 percent of respondents believe their companies are too small to be the target of ransomware. This has remained unchanged since 2017.

Ponemon Institute surveyed 659 IT and IT security professionals in small to large-sized companies in the United States. All respondents have responsibility for containing ransomware infections within their organization.

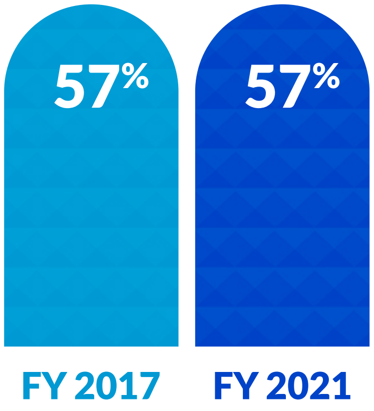


Figure 1. My company believes it is too small to be the target of ransomware

Strongly Agree and Agree responses reported

The following findings describe the costs and consequences of a ransomware attack.

- Of the 80 percent of companies that experienced one or more ransomware attacks, 53 percent of respondents say the ransom was paid and averaged over $1 million. The preferred methods of payment are bitcoin and virtual currencies.
- If companies didn't pay a ransom, it was because they had a full and accurate backup. However, respondents also believe a full and accurate backup is not enough when experiencing a ransomware attack.
- Of the companies that paid the ransom, it was because they could not afford the downtime and had a cyber insurance policy that covered the financial consequences of a ransomware attack. Fifty percent of respondents say the cybercriminals provided a decryption key.
- Companies suffered financial consequences such as having to shut down for a period of time, losing customers, and eliminating jobs.
- According to the research, an average of 14 staff members each spent 190 hours to contain and remediate their companies' largest ransomware incident. Based on an average hourly rate of $63.50, the average cost to assign staff to deal with the incident was approximately $170,000.
- The highest total costs resulting from a ransomware attack are from legal and regulatory actions, followed by the cost resulting from the company's response to information misuse or theft.
- Cybercriminals were most likely to use phishing/social engineering and insecure websites to unleash ransomware. The most compromised devices are desktops and laptops; however, since 2017, mobile devices have been increasingly being targeted.

Over $1 million paid on average, typically in bitcoin or other virtual currencies

- Compromised devices infected other devices in the network. Very often, data was exfiltrated from the device.

- As in the previous study, companies are reluctant to report the incident to law enforcement because of concerns about negative publicity and the potential loss of customers.

Following are the key takeaways from this research.

IoT risk awareness is rising and ransomware prevention is increasingly prioritized. Since 2017, awareness of IoT risks has risen from 58 percent of respondents in 2017 to 67 percent of respondents in this year's research. Prevention of ransomware is becoming more of a priority, increasing 46 percent to 53 percent. Respondents say that if companies are attacked their organizations are slightly less likely to pay the ransom since 2017.

There is a lack of confidence in security controls. Companies spend an average of $6 million annually on staff and technologies meant to prevent, detect, contain and resolve ransomware attacks. However, there is only a slight improvement in confidence about security controls that prevent ransomware attacks.

Companies are increasingly relying upon third parties to deal with the prevention and consequences of a ransomware attack. Since 2017, the engagement of third parties to reduce the risk increased significantly from 58 percent of respondents to 69 percent of respondents. To remediate the incident, the use of the expertise of third parties has increased from 59 percent of respondents to 70 percent of respondents.

Despite the seriousness of ransomware, the ability to respond is low. As reported, the increase in ransomware attacks has been significant since 2017. However, the ability to respond to such attacks is very low. Companies must assess their staff, technologies, and policies to increase overall readiness.

The severity of ransomware infections has increased over the past 12 months. Sixty-one percent of respondents say the severity of ransomware infections has significantly increased (25 percent) or increased (36 percent) since last year. In 2017, 57 percent of respondents said the severity of ransomware infections increased significantly (18 percent) or increased (39 percent) over the past 12 months.

Companies have been receiving more ransomware alerts since 2017. As defined in this research, a ransomware alert is a notice that your system may be targeted or susceptible to a ransomware attack. These alerts are communicated via threat intelligence and law enforcement.

The number of weekly alerts has increased from 25 weekly alerts in 2017 to 34 in this year's study. In 2017, 46 percent of these alerts were considered reliable. In this year, 51 percent are considered reliable. In a typical month, an average of 6 percent of attempted attacks trigger an alert through one or more security controls but remain undetected.

A full and accurate backup is not considered enough by 55 percent of respondents. As discussed previously, only 32 percent of respondents are confident in their security controls, indicating the need to use more effective technologies to prevent ransomware attacks.

More companies need to conduct security assessments as part of their ransomware readiness strategy. Only about half (51 percent) of respondents say their organizations regularly conduct assessments to test their ransomware prevention and recovery practices.

In some cases, cyber insurance providers are decreasing their coverage for ransomware attacks. Most companies (64 percent of respondents) do not have cyber insurance policies that cover ransomware. Of the 36 percent of respondents who say their policies cover such attacks, 40 percent say the cyber insurance provider modified its ransomware protection resulting in decreased coverage. The average annual premium for a cyber insurance policy is $17,100.

Employees are still considered the weakest link in preventing ransomware attacks. Despite employee security training awareness programs that address social engineering, spear phishing and ransomware attacks, only 30 percent of respondents are very confident (12 percent) or confident (18 percent) in their employees' ability to detect social engineering lures that could result in a ransomware attack.

Despite the risk, only half of training programs fully cover social engineering, spear phishing and ransomware. Sixty-one percent of respondents say their companies conduct continuous employee security awareness training. Of these respondents, 92 percent say the training covers social engineering, spear phishing and ransomware attacks fully (50 percent of respondents) or some coverage (42 percent of respondents).

In addition to insider risks, companies face ransomware threats from their suppliers and third parties. Seventy-five percent of respondents say they are very concerned about the risks the supply chain poses to their company as they relate to ransomware. Only 33 percent of respondents say third parties have the necessary privacy and security practices in place to reduce the risk of a data breach involving their companies' sensitive and confidential information.

To reduce the risk of ransomware attacks, companies need to assess the security and privacy practices of their supply chain and third parties. As discussed, 75 percent of respondents are concerned about the ransomware risks posed by third parties. However, only 36 percent of respondents say their organizations evaluate third parties' security and privacy practices. Of those, only slightly more than half (53 percent) of respondents say their organizations conduct an assessment of the third party's security and privacy practices. Currently, organizations mainly rely upon a review of written policies and procedures, according to 64 percent of respondents.

PART TWO

Key Findings

In this section of the report, we provide an analysis of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Companies lack the readiness to respond to ransomware attacks
- Phishing and the insider ransomware risk
- Third-party and supply chain ransomware risks
- The ransomware experience—extortion and escalation
- The cost and consequences of ransomware attacks

Companies lack the readiness to respond to ransomware attacks

IoT devices are increasing the risk of ransomware. As shown in Figure 2, awareness of the risks created by IoT devices has increased from 58 percent of respondents in 2017 to 67 percent of respondents in this year's research. However, ransomware prevention is becoming more of a priority, increasing from 46 percent to 53 percent. If companies are attacked, respondents say their organizations are slightly less likely to pay the ransom since 2017.

Companies spend an average of $6 million annually on staff and technologies meant to prevent, detect, contain and resolve ransomware attacks. However, there is only a slight improvement in confidence about security controls that prevent ransomware attacks.

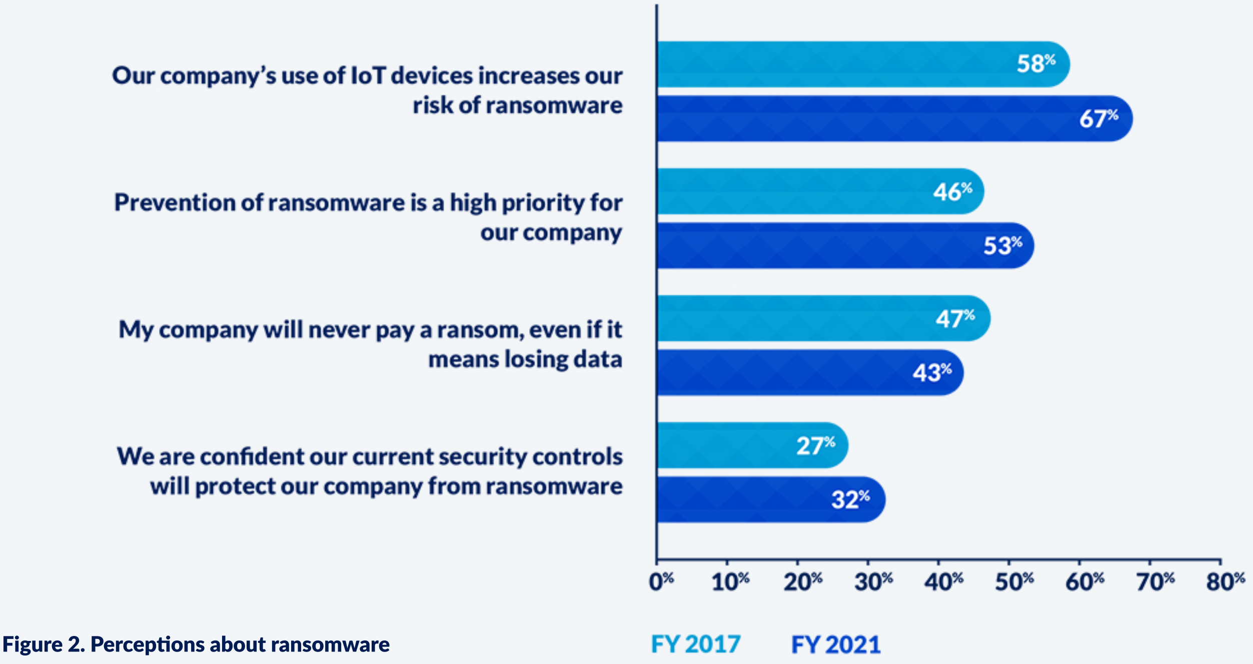


Figure 2. Perceptions about ransomware

Strongly Agree and Agree responses combined

To deal with the prevention and consequences of a ransomware attack, companies are increasingly relying upon third parties. According to Figure 3, since 2017, the engagement of third parties to reduce the risk increased significantly from 58 percent of respondents to 69 percent of respondents. To remediate the incident, the use of the expertise of third parties has increased from 59 percent of respondents to 70 percent of respondents.

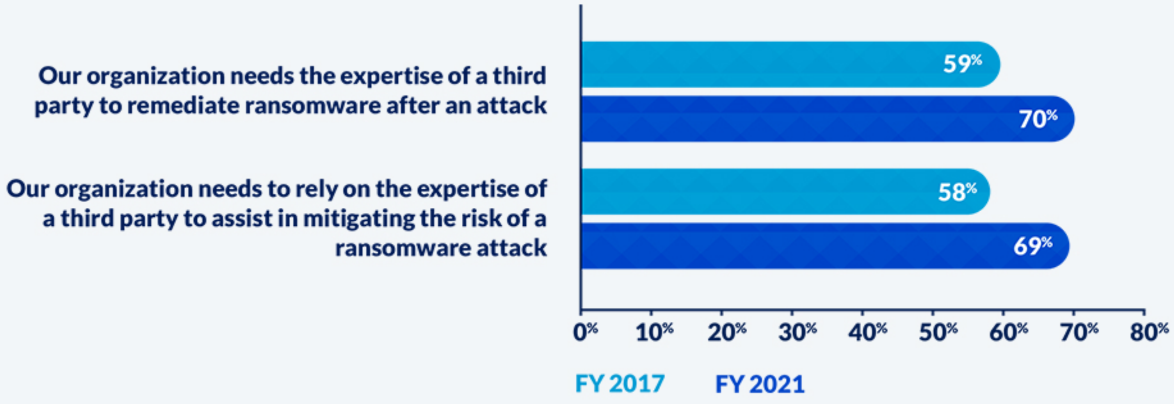


Figure 3. Third parties are becoming more important in managing ransomware risks

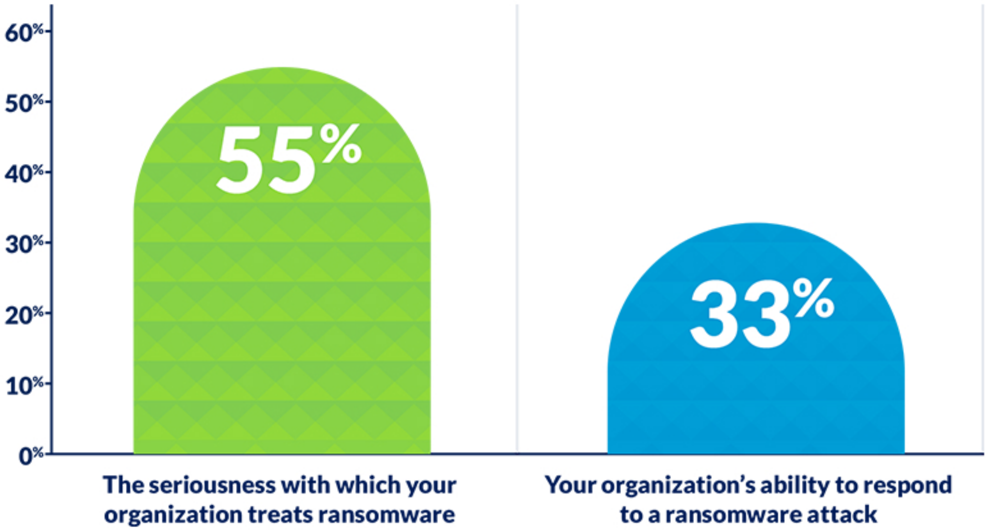
Strongly Agree and Agree responses combined

Despite the seriousness of ransomware, the ability to respond is low. Respondents were asked to rate the seriousness with which their companies treat ransomware on a scale of 1 = not serious to 10 = extremely serious. As reported, the increase in ransomware attacks has risen significantly since 2017. However, the ability to respond to such attacks is very low. As a result, it is critical that companies assess the ability of their staff, technologies and policies to improve readiness.

Figure 4 presents the very or extremely serious ransomware responses (55 percent of respondents). When asked to rate their companies' ability to respond to ransomware attacks on a scale from 1 = no ability to 10 = high ability, only 33 percent of respondents rate their companies' ability as high.

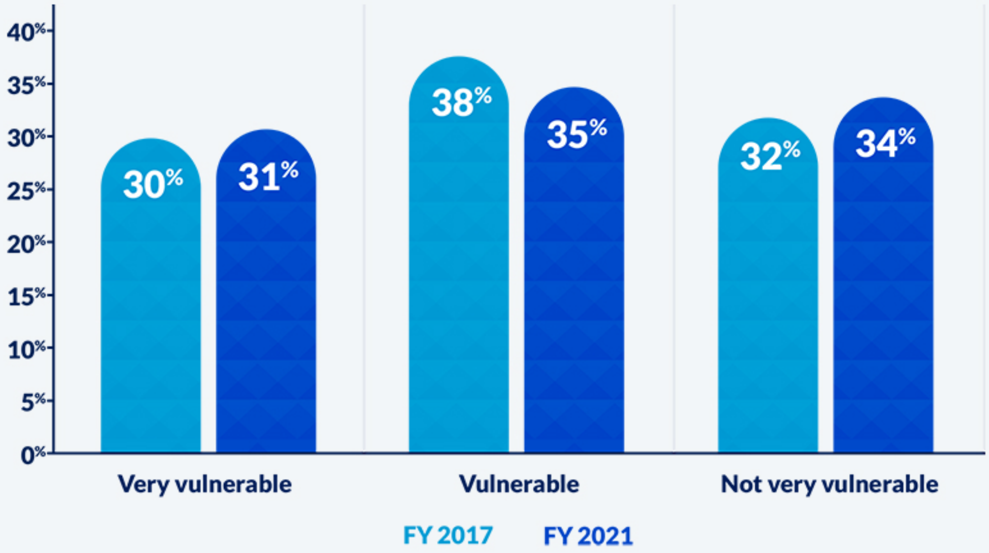
Figure 4. The ransomware seriousness and ability to respond gap

On a scale from 1 = not serious/no ability to 10 = extremely serious/high ability
7+ responses shown



Companies continue to believe they are very vulnerable or vulnerable to a ransomware attack. In 2017, 68 percent of respondents, as shown in Figure 5, believed their company was very vulnerable (30 percent) or vulnerable (38 percent) to a ransomware attack. According to this year's research, 66 percent of respondents say their organizations are very vulnerable or vulnerable to a ransomware attack.

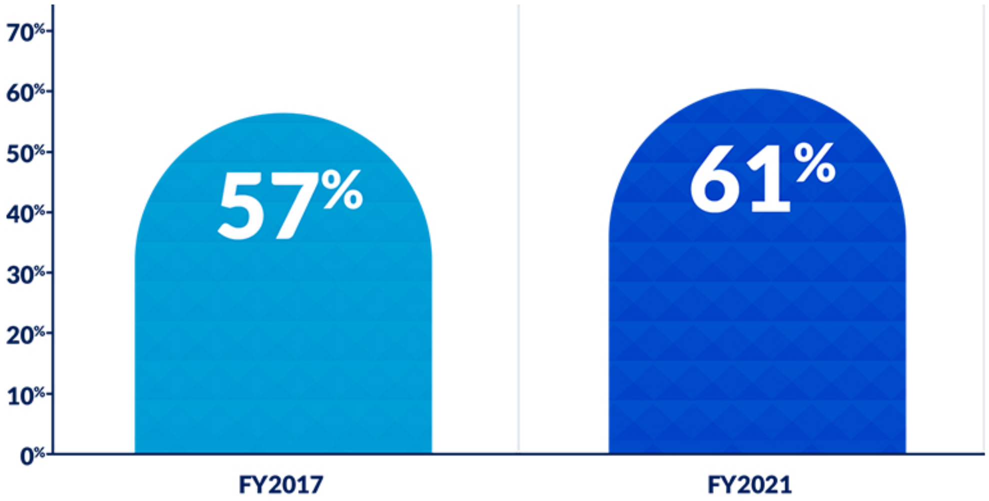
Figure 5. How vulnerable do you feel your company is to a ransomware attack over the next 12 months?



The severity of ransomware infections has increased over the past 12 months. According to Figure 6, 61 percent of respondents say the severity of ransomware infections has significantly increased (25 percent) or increased (36 percent) since last year. In 2017, 57 percent said the severity of ransomware infections increased significantly (18 percent) or increased (39 percent) over the past 12 months.

Figure 6. How has the severity of ransomware infections changed over the past 12 months?

Significantly increase and Increase responses combined

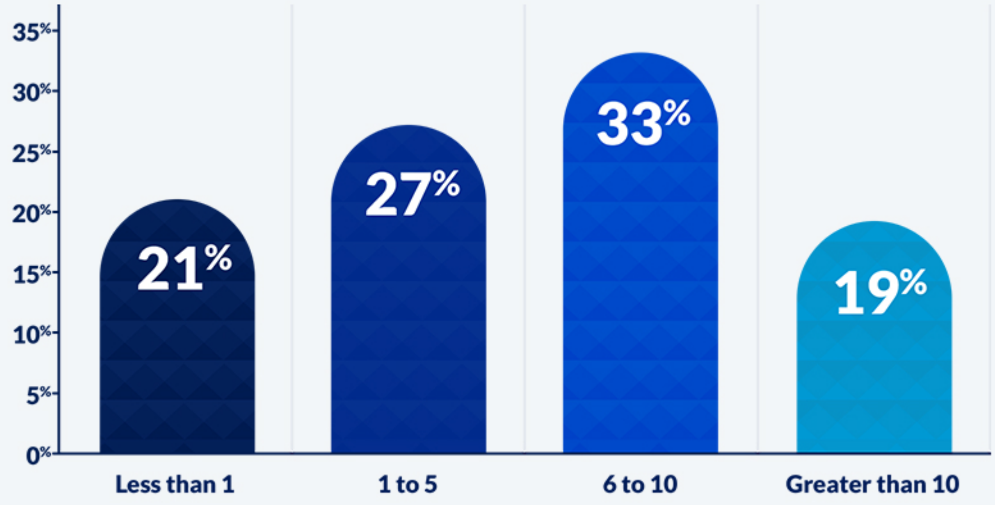


Companies have been receiving more ransomware alerts since 2017. As defined in this research, a ransomware alert is a notice that your system may be targeted or susceptible to a ransomware attack. These alerts are communicated via threat intelligence and law enforcement.

The number of weekly alerts has increased from 25 weekly alerts in 2017 to 34 in this year's study. In 2017, 46 percent of these alerts were considered reliable and this year 51 percent are considered reliable. As shown in Figure 7, in a typical month, an average of 6 percent of attempted attacks trigger an alert through one or more security controls but remain undetected.

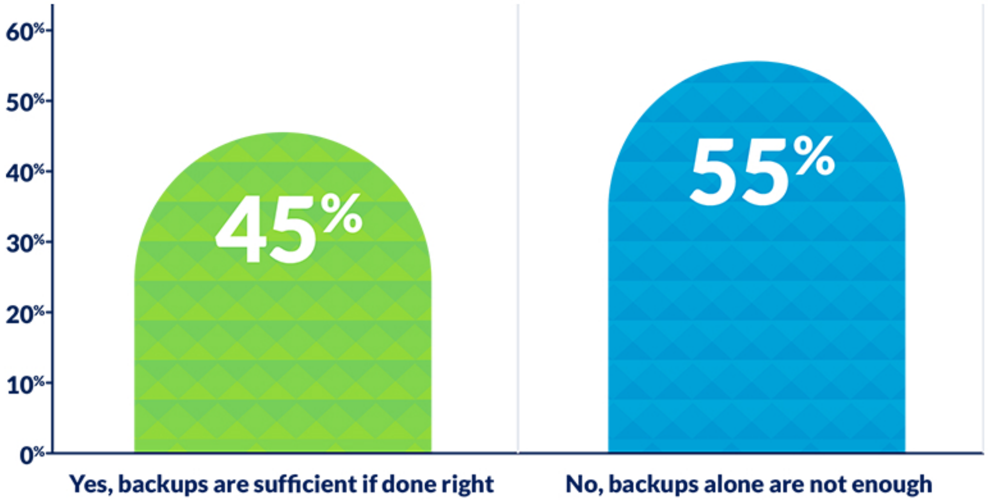
Figure 7. How many attempted attacks trigger an alert through one or more security controls but are undetected?

Extrapolated value = 6%



A full and accurate backup is not considered enough by 55 percent of respondents. As discussed previously, only 32 percent of respondents are confident in their security controls, indicating the need to use more effective technologies to prevent ransomware attacks.

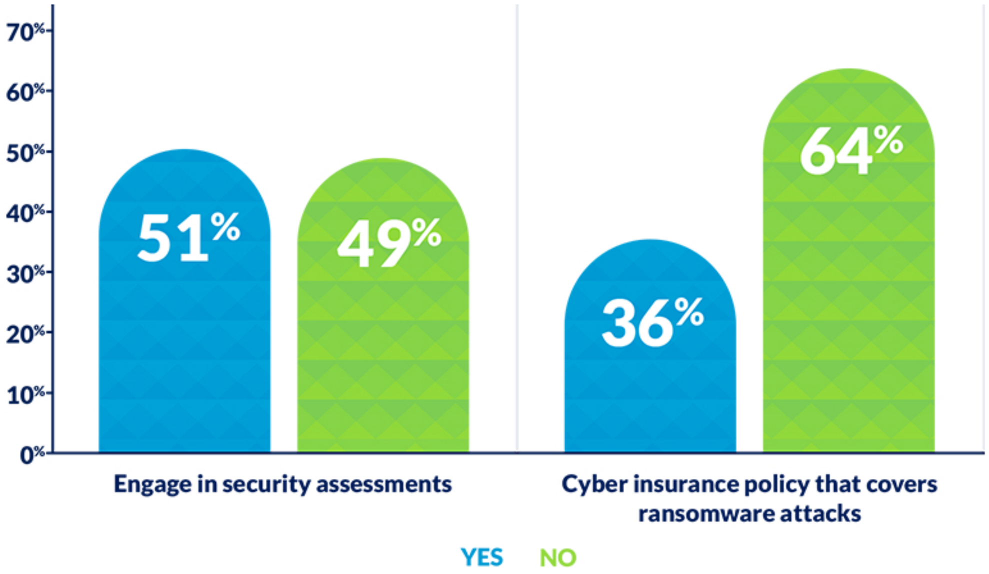
Figure 8. Do you think having a full and accurate backup is a sufficient defense against ransomware?



More companies need to conduct security assessments as part of their ransomware readiness strategy. Only about half (51 percent) of respondents say their organizations regularly conduct assessments to test their ransomware prevention and recovery practices, as shown in Figure 9.

In addition, most companies (64 percent of respondents) do not have cyber insurance policies that cover ransomware. Of the 36 percent of respondents who say their policies cover such attacks, 40 percent say the cyber insurance provider modified its ransomware protection resulting in decreased coverage. The average annual premium for a cyber insurance policy is $17,100.

Figure 9. Do organizations conduct security assessments and purchase cyber insurance that covers ransomware attacks?



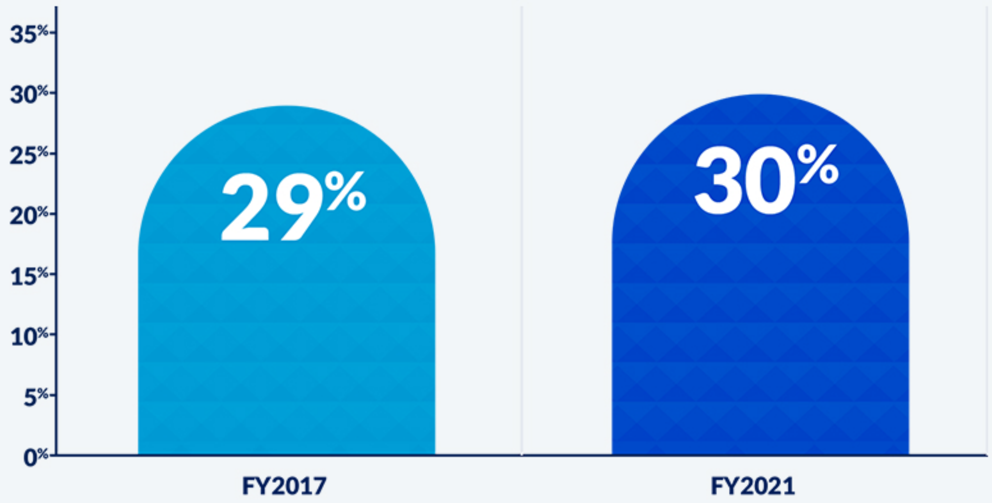
Phishing and the insider ransomware risk

Employees are still considered the weakest link in preventing ransomware attacks. Despite employee security training awareness programs that address social engineering, spear phishing and ransomware attacks, only 30 percent of respondents are very confident (12 percent) or confident (18 percent) in their employees' ability to detect social engineering lures that could result in a ransomware attack. This perception has been virtually unchanged since 2017.

Only about half of companies say their training programs fully address the risks of phishing, social engineering and ransomware attacks. Sixty-one percent of respondents say their companies conduct continuous employee security awareness training. Of these respondents, 92 percent say the training covers social engineering, spear phishing and ransomware attacks fully (50 percent of respondents) or some coverage (42 percent of respondents).

Figure 10. How confident are you in your employees' ability to detect social engineering lures that could result in a ransomware attack?

Very confident and Confident responses combined



Third party and supply chain ransomware risks

In addition to insider risks, companies face ransomware threats from their suppliers and third parties. Respondents were asked to rate their concern and confidence in the security and privacy practices of their third parties and suppliers on a scale of 1 = no concern/confidence to 10 = highly concerned/highly confident.

As shown in Figure 11, 75 percent of respondents say they are very concerned about the risks the supply chain poses to their organization as it relates to ransomware. Only 33 percent of respondents say third parties have the necessary privacy and security practices in place to reduce the risk of a data breach involving their organizations' sensitive information.

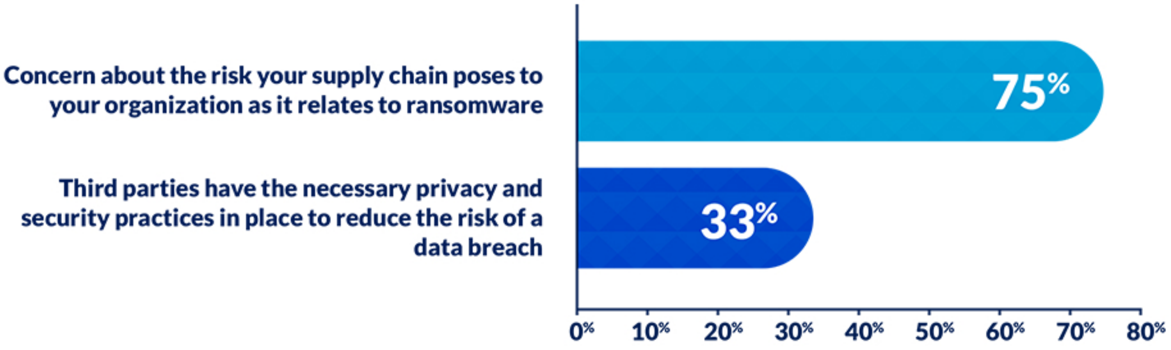


Figure 11. Concern and lack of confidence in third parties and suppliers

On a scale from 1 = no concern/no confidence to 10 = highly concerned/highly confident, 7+ responses presented

To reduce the risk of ransomware attacks, companies need to assess the security and privacy practices of their supply chain and third parties. As discussed, 75 percent of respondents are concerned about the ransomware risks posed by third parties. However, only 36 percent of respondents say their organizations evaluate third parties' security and privacy practices.

Figure 12 presents a list of activities used to ensure the sharing of confidential information is secure. Of these respondents, slightly more than half (53 percent) of respondents say their organizations conduct an assessment of the third party's security and privacy practices. Currently, organizations mainly rely upon a review of written policies and procedures according to 64 percent of respondents.

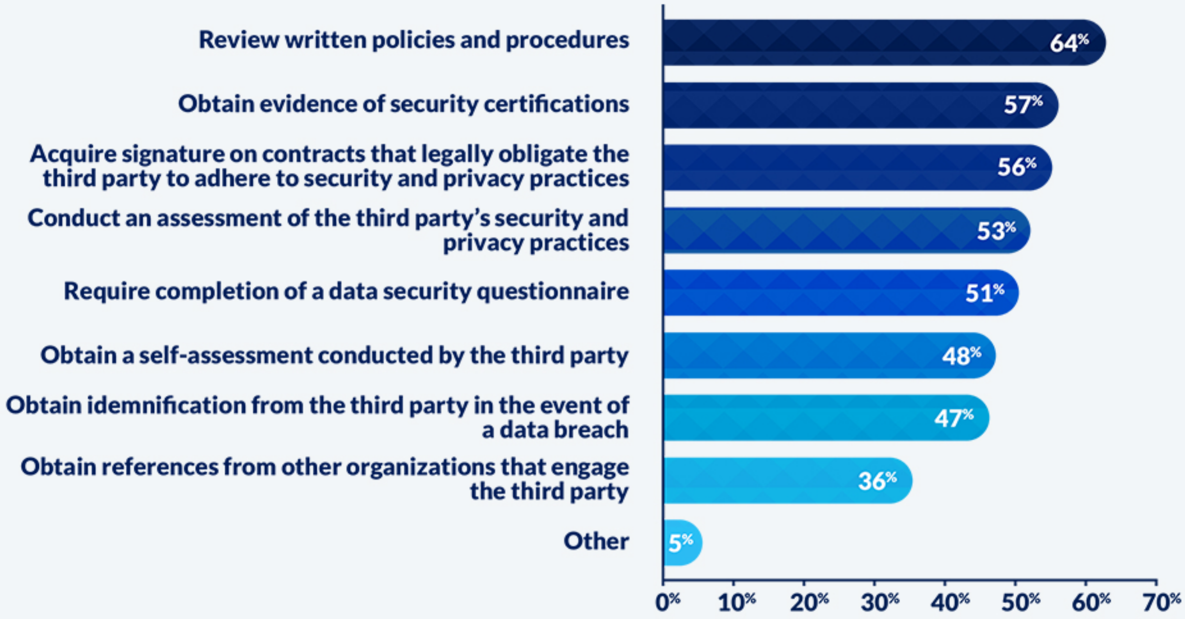


Figure 12. How does your organization evaluate third-parties' security and privacy practices before engaging them?

More than one response permitted

The ransomware experience—extortion and escalation

The following findings are based on the 80 percent of respondents who say that their companies experienced ransomware, an increase from 51 percent in the previous research.

Most companies experience encrypting ransomware.[2] As shown in Figure 13, 80 percent of respondents had a ransomware incident within the past three months to more than one year ago. In 2017, 51 percent of respondents reported a ransomware attack.

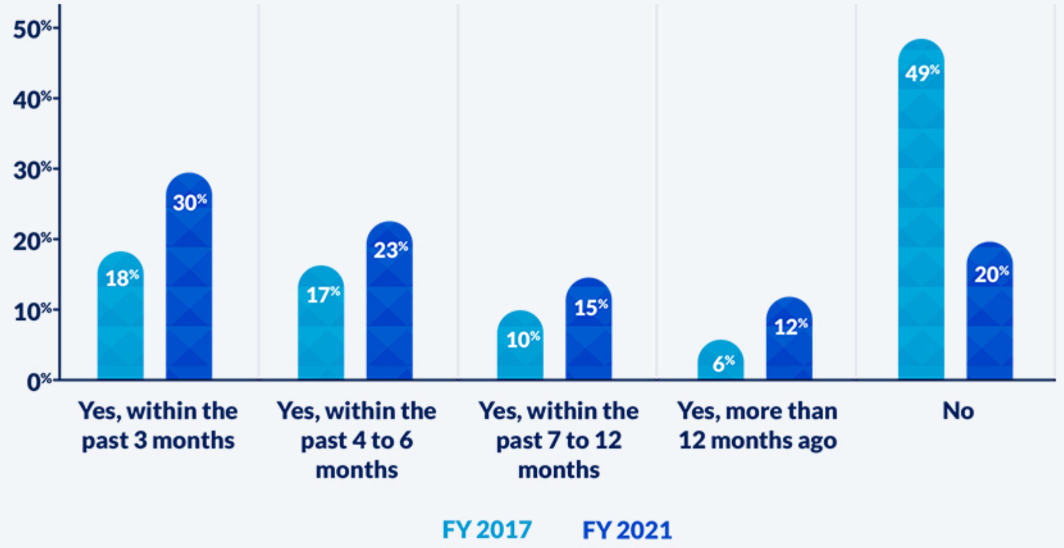


Figure 13. Has your company experienced one or more ransomware attacks?

On average, in this year's study, 60 percent of respondents say their companies had a crypto-ransomware attack, 21 percent of respondents say it was locker ransomware and 19 percent of respondents say they experienced both crypto and locker type attacks. Both companies and their suppliers had an average of 5 ransomware incidents in the past year, as shown in Figure 14.

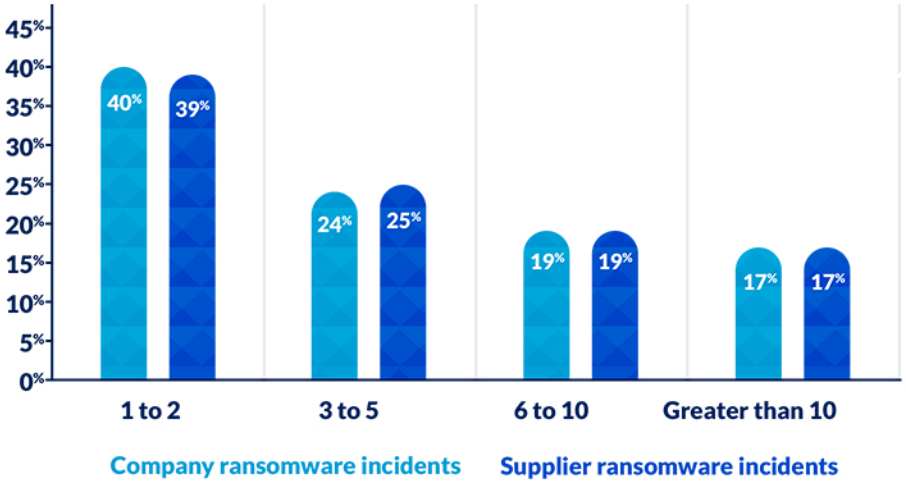


Figure 14. How many ransomware incidents have your company and suppliers experienced?

Extrapolated value for company and supplier = 5.0

[2] Encrypting ransomware incorporates advanced encryption algorithms. It's designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content. Examples include CryptoLocker, CryptoWall and more. Locker ransomware locks the victim out of the operating system, making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer. An example includes Winlocker.

Companies should be aware that attackers use a variety of extortion tactics to pressure companies. As shown in Figure 15, 31 percent of respondents say the attacker used single (encryption), followed by data exfiltration (27 percent of respondents) and DDoS (25 percent of respondents).

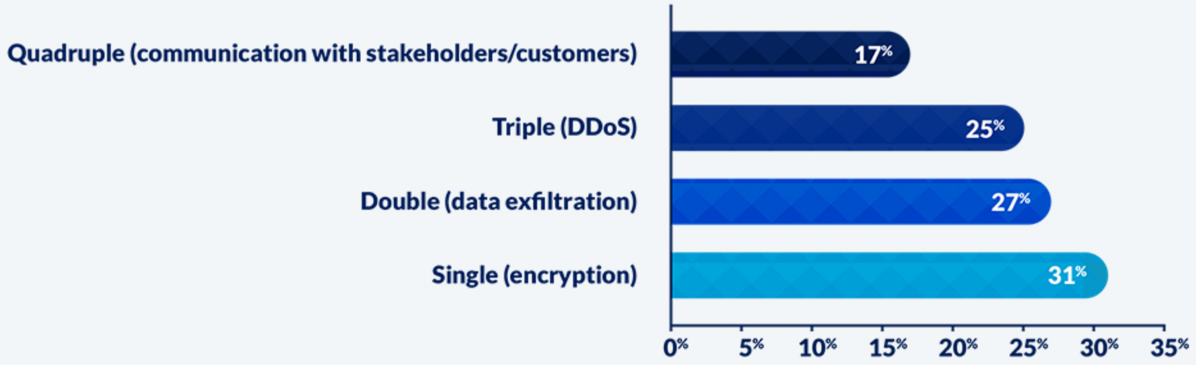


Figure 15. Which extortion tactic did the attackers use to exert pressure?

Training insiders to detect a phishing attack would mitigate the threat of ransomware. It was previously reported that most respondents are not confident in their employees' ability to detect a phishing or other social engineering attempt. Consequently, almost half of all ransomware attacks (48 percent of respondents) were due to phishing, as shown in Figure 16. Phishing is followed by a Remote Desktop Protocol (RDP) compromise (34 percent of respondents) to remotely connect to unsecured RDP services.

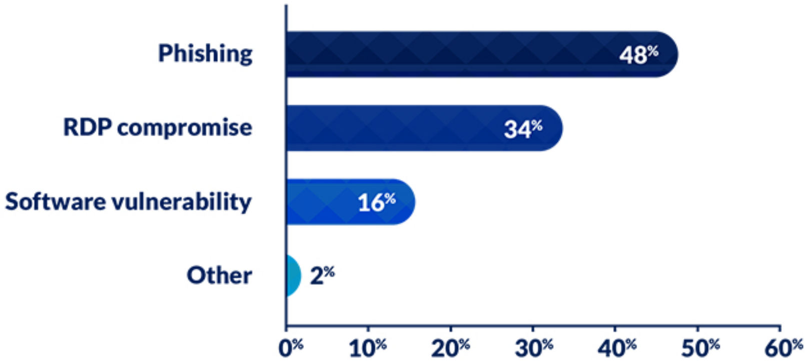


Figure 16. How was the ransomware unleashed?

The most vulnerable devices are desktop/laptop devices and servers. According to Figure 17, attackers are primarily going after the desktop/laptops, followed by servers. However, more attackers have been targeting mobile devices since 2017. Of those respondents who selected desktop/laptop or mobile devices, 52 percent say the device was used for personal and business purposes.

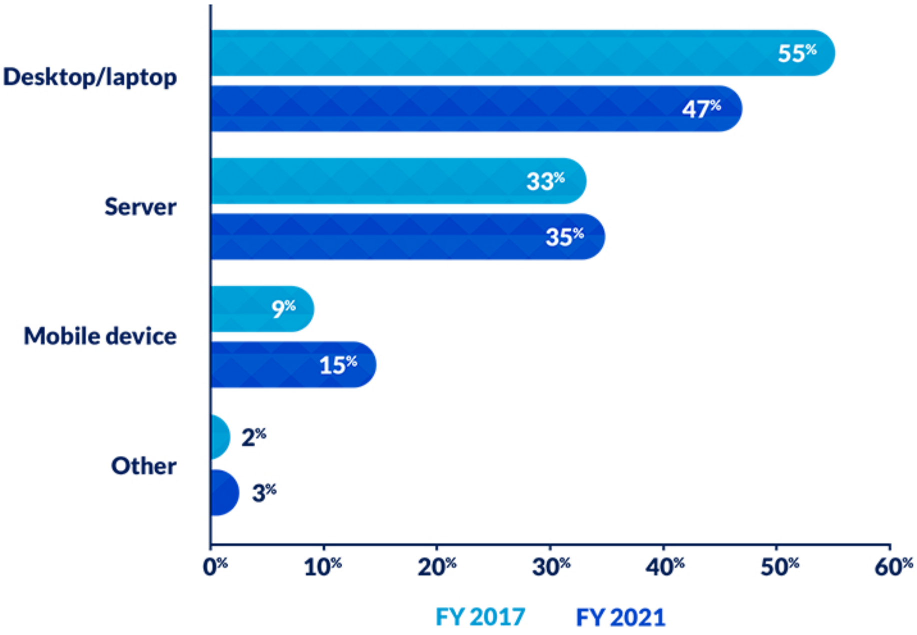


Figure 17. Which type of device was compromised by ransomware?

Ransomware attacks can infect other devices in the network. Fifty-two percent of respondents say the compromised desktop/laptop or mobile device infected other devices in the network (e.g., lateral infection). According to Figure 18, the most vulnerable areas for lateral movement are weak passwords on high privileged accounts such as service and administrative accounts (45 percent of respondents), followed by cached credential attacks (42 percent of respondents).

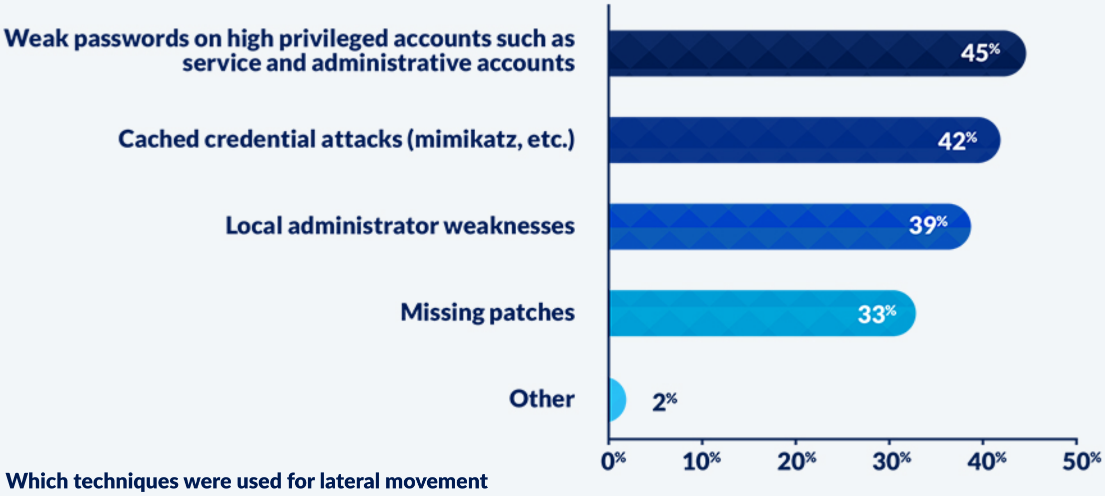
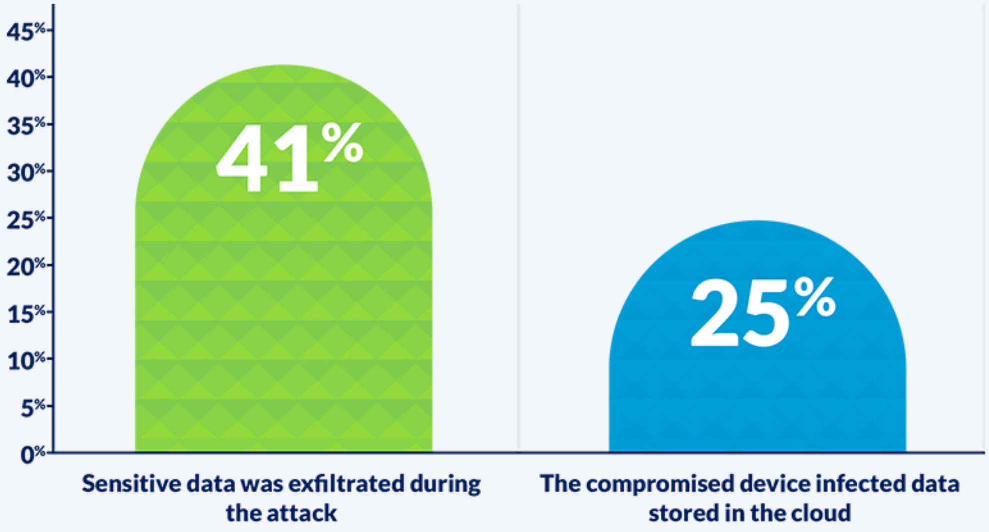


Figure 18. Which techniques were used for lateral movement and privilege escalation? More than one response permitted

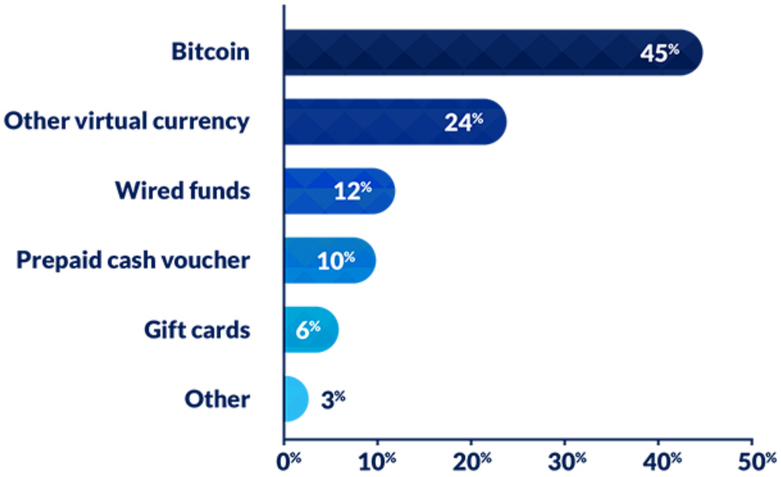
Forty-one percent of respondents say the attack resulted in the exfiltration of sensitive data, and 25 percent say the compromised device infected data stored in the cloud, as shown in Figure 19.

Figure 19. The impact of the attack on sensitive data



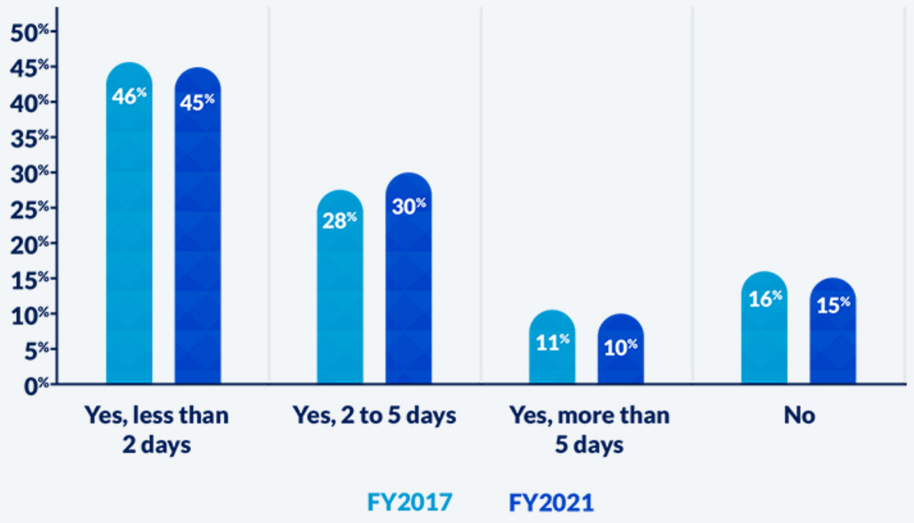
Bitcoin and virtual currencies are the preferred methods of payment. The average payment was approximately $1 million, and according to 69 percent of respondents, the payment methods of choice are bitcoin (45 percent) or other virtual currency (24 percent), as shown in Figure 20.

Figure 20. In what format was payment demanded?



Companies face enormous pressure to pay the ransom. Most companies had less than two to five days to make the payment, as shown in Figure 21. Fifty-four percent of respondents say the attacker demanded the payment within the deadline or it would be increased.

Figure 21. Did the threat actor impose a time limit for payment?



More companies have been paying the ransom since 2017. Specifically, in this year's research, 53 percent of respondents say their companies paid the ransom, increasing from 48 percent in 2017.

The 47 percent of respondents that did not pay the ransom (a decrease from 52 percent in 2017) were asked why they decided not to pay. According to Figure 22, the primary reason for not paying includes having an effective backup strategy. However, this decreased from 42 percent to 39 percent of respondents. Another reason given was that the compromised data wasn't critical. This increased from 14 percent of respondents to 18 percent of respondents in this year's study.

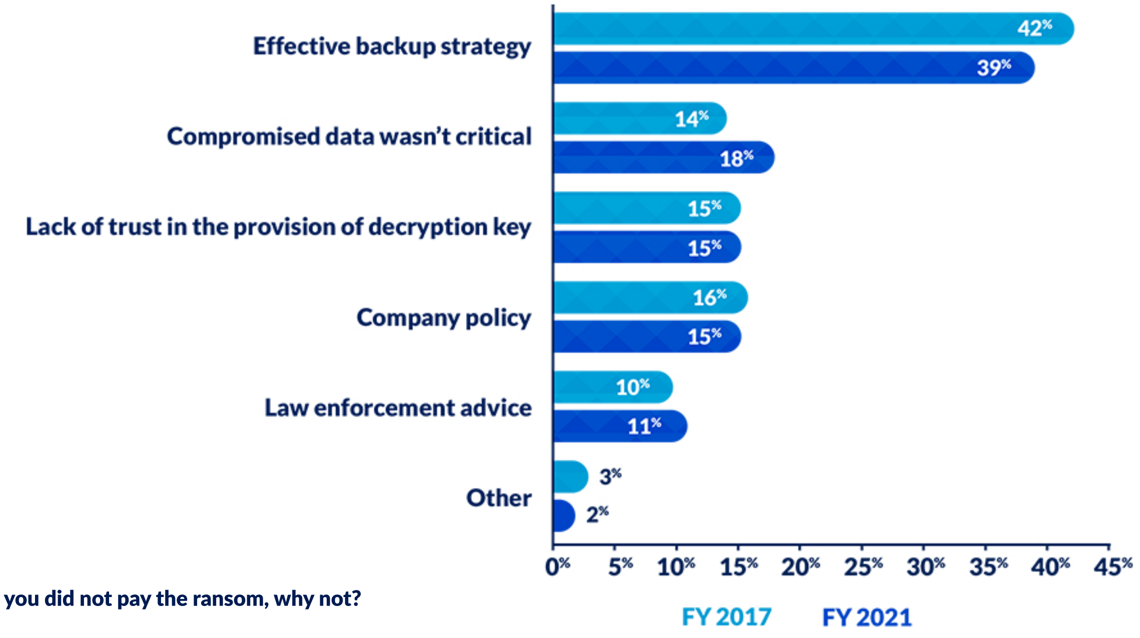


Figure 22. If you did not pay the ransom, why not?

Avoiding downtime and having a cyber insurance policy that covers ransomware attacks are reasons to pay the ransom. Understandably, many companies cannot afford downtime and that is the number one reason for paying the ransom, as shown in Figure 23. Thirty-three percent of respondents say their organizations did pay because they had a cyber insurance policy that covered ransomware attacks.

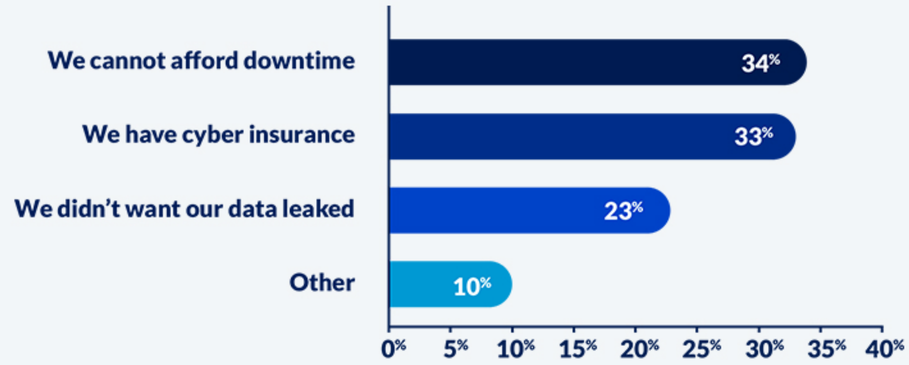


Figure 23. If you paid the ransom, why did your organization do so?

Fear of losing customers deters companies from reporting the attack. Concerns about adverse publicity (49 percent of respondents) prevent companies from reporting the incident to law enforcement, as shown in Figure 24.

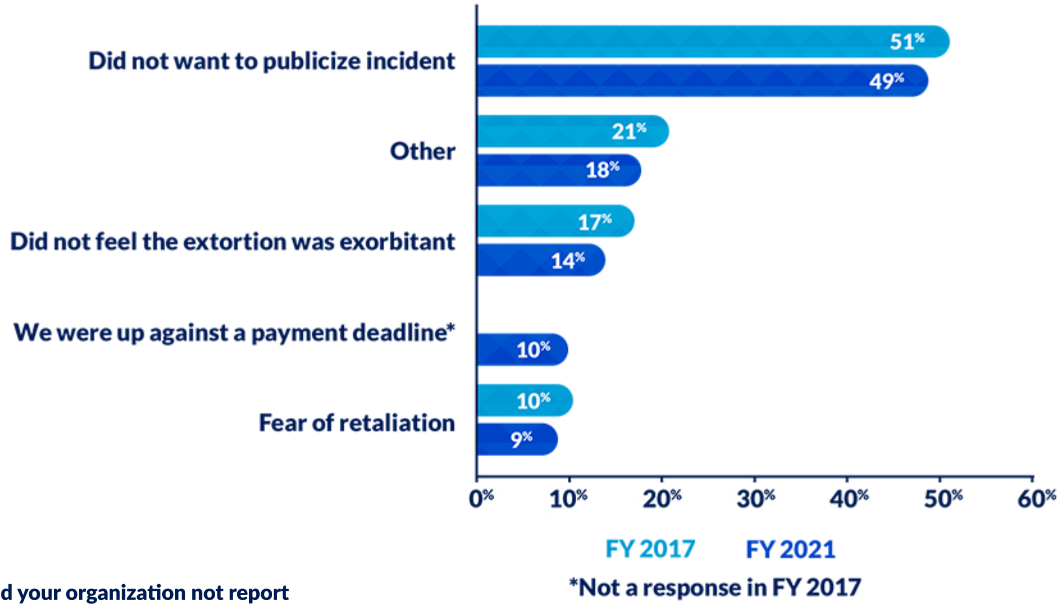


Figure 24. Why did your organization not report the incident to law enforcement?

The cost and consequences of a ransomware attack

A ransomware attack has severe consequences for small to large-sized companies. As shown in Figure 25, in the aftermath of an attack, 45 percent of respondents had to shut down their company and 40 percent of respondents said their company lost customers.

According to the research, 14 staff members each spent an average of 190 hours to contain and remediate their companies' largest ransomware incident. Based on an average hourly rate of $63.50, the average cost to assign staff to deal with the incident was approximately $170,000.

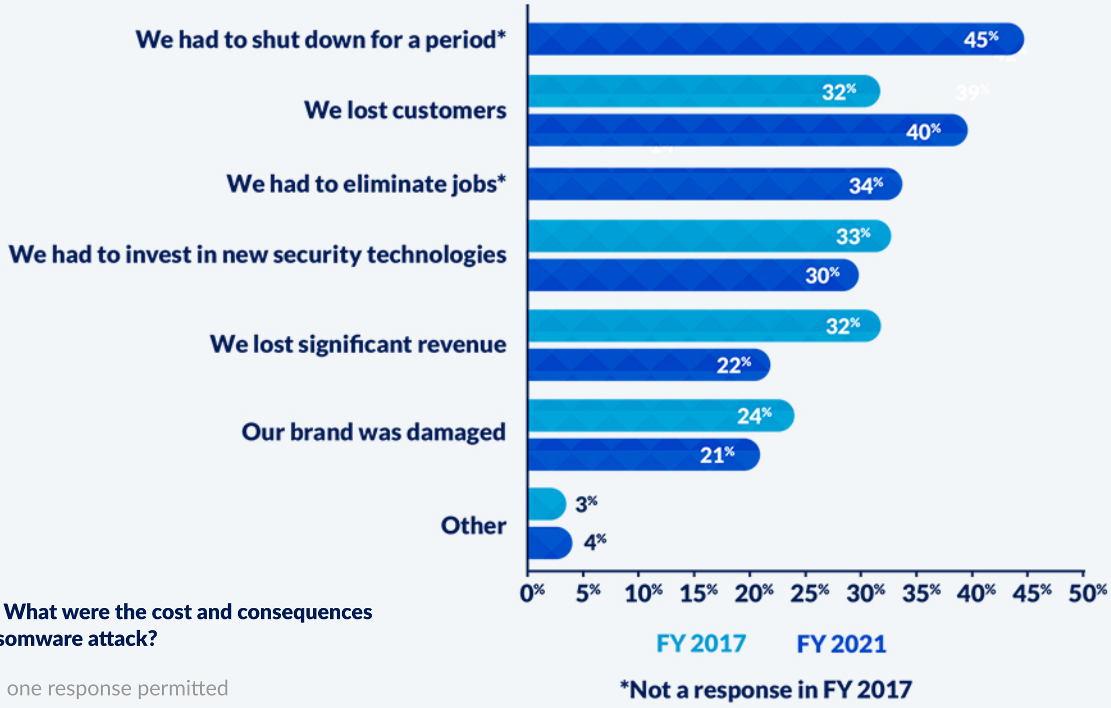


Figure 25. What were the cost and consequences of the ransomware attack?

More than one response permitted

If a company has a ransomware attack, the highest costs are from legal and regulatory actions. Respondents were asked to rate the most significant financial impact caused by a ransomware attack from 1 = most significant to 6 = least significant financial impact. As shown in Table 1, the most significant financial impact is caused by legal and regulatory actions followed by the cost of users' idle time and lost productivity because of IT security failure. The least impactful expense is lost income or revenues due to IT security failures.

Table 1. Six cost categories for a ransomware attack
Ranked 1 = most significant financial impact and 6 = least significant financial impact.

	Ranking
Cost associated with legal and regulatory actions	1.65
Cost of users' idle time and lost productivity because of IT security failure	2.25
Cost resulting from the organization's response to information misuse or theft	2.36
Cost of technical support, including forensics and investigative operations	3.34
Cost associated with reputation and brand damage because of IT security failure	3.89
Revenues or income lost because of IT security failure	4.58

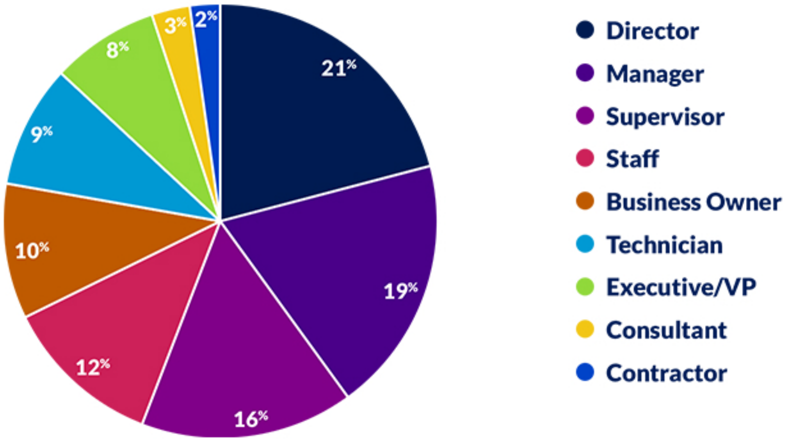
PART THREE

Methods

A sampling frame composed of 15,577 individuals in the United States responsible for containing ransomware infections within their organization were selected for participation in this survey. As shown in Table 2, 716 respondents completed the survey. Screening removed 57 respondent surveys. The final sample was 659 respondent surveys (or a 3.7 percent response rate).

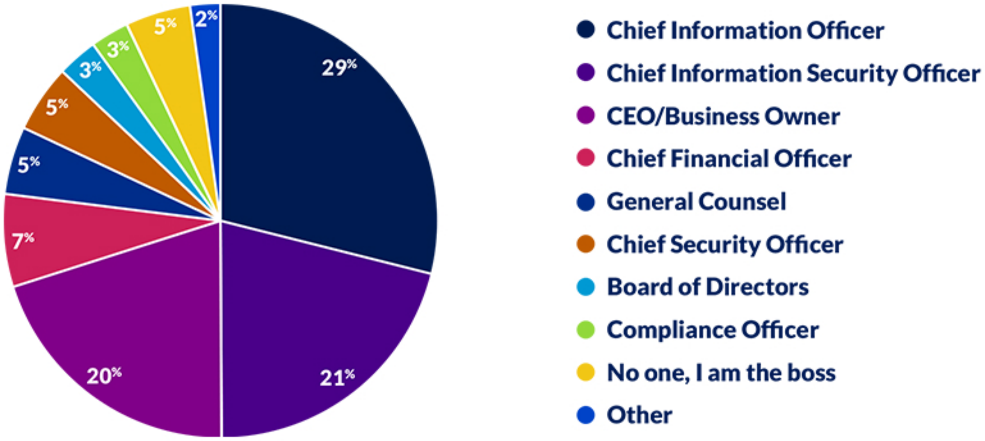
Table 2. Sample response	Freq	Pct%
Total sampling frame	17,577	100.0%
Total returns	716	4.1%
Rejected surveys	57	0.3%
Final sample	659	3.7%

Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half (56 percent) of the respondents are at or above the supervisory levels.



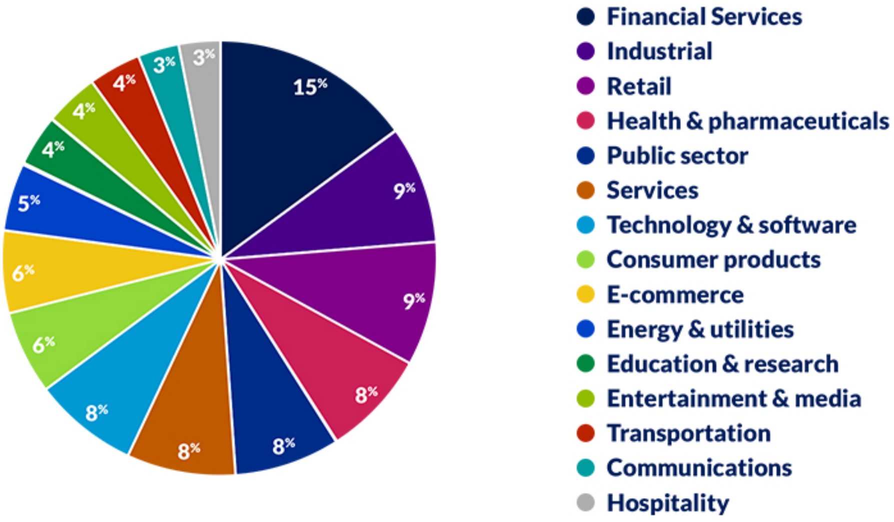
Pie Chart 1. Position level within the organization

As shown in Pie Chart 2, 29 percent of respondents report directly to the chief information officer, 21 percent report to the chief information security officer and 20 percent of respondents report to the CEO/business owner.



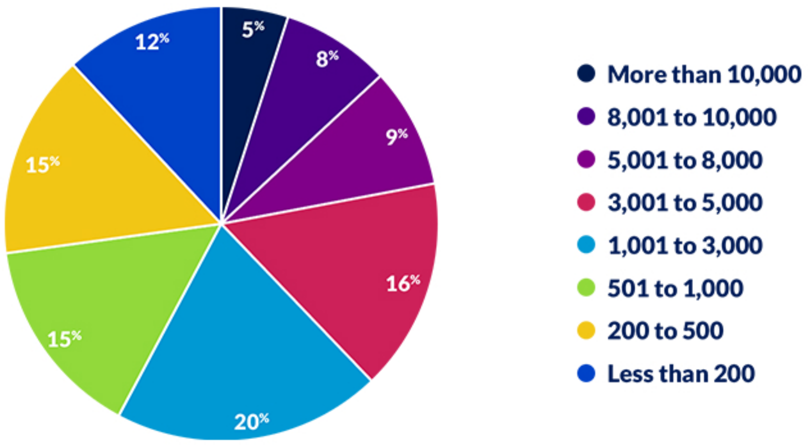
Pie Chart 2. The primary person reported to within the organization

Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (15 percent of respondents) as the largest segment, including banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by industrial and retail (each at 9 percent of respondents), health and pharmaceuticals, public sector, services, and technology and software (each at 8 percent of respondents).



Pie Chart 3. Primary industry focus

According to Pie Chart 4, 58 percent of the respondents are from organizations with a global headcount of more than 1,000 employees.



Pie Chart 4. Worldwide headcount of the organization

PART FOUR

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

Non-response bias:

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias:

The accuracy is based on contact information and the degree to which the list is representative of individuals who have responsibility for containing ransomware infections within their organization. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results:

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Detailed Survey Results

The following tables provide the frequency or percentage of responses to all survey questions in this study. All survey responses were captured in October 2021.

Survey response	FY2021	Pct%
Total sampling frame	17,577	100.0%
Total returns	716	4.1%
Rejected surveys	57	0.3%
Final sample	659	3.7%

Part 1. Screening questions

S1. Does your role include responsibility for addressing ransomware attacks?	FY2021	FY2017
Yes, full responsibility	41%	33%
Yes, some responsibility	45%	50%
Yes, minimum responsibility	16%	18%
No responsibility (Stop)	0%	0%
Total	102%	100%

Part 2. Attributions: Please rate each statement using the agreement scale below the item.

Q1a. My company believes it is too small to be the target of ransomware.	FY2021	FY2017
Strongly agree	20%	22%
Agree	37%	35%
Unsure	23%	21%
Disagree	15%	16%
Strongly disagree	5%	6%
Total	100%	100%

Q1b. My company will never pay a ransom, even if it means losing data.	FY2021	FY2017
Strongly agree	16%	19%
Agree	27%	28%
Unsure	21%	21%
Disagree	26%	22%
Strongly disagree	10%	10%
Total	100%	100%

Q1c. Prevention of ransomware is a high priority for our company.	FY2021	FY2017
Strongly agree	27%	18%
Agree	26%	28%
Unsure	19%	22%
Disagree	21%	20%
Strongly disagree	7%	12%
Total	100%	100%

Q1d. Our company's use of IoT devices increases our risk of ransomware.	FY2021	FY2017
Strongly agree	30%	22%
Agree	37%	36%
Unsure	19%	18%
Disagree	9%	17%
Strongly disagree	5%	6%
Total	100%	100%

Q1e. We are confident our current security controls will protect our company from ransomware.	FY2021	FY2017
Strongly agree	11%	9%
Agree	21%	18%
Unsure	28%	26%
Disagree	26%	32%
Strongly disagree	14%	15%
Total	100%	100%

Q1f. Our organization needs to rely on the expertise of a third party to assist in mitigating the risk of a ransomware attack.	FY2021	FY2017
Strongly agree	32%	23%
Agree	37%	35%
Unsure	14%	17%
Disagree	10%	19%
Strongly disagree	7%	6%
Total	100%	100%

Q1g. Our organization needs the expertise of a third party to remediate ransomware after an attack.	**FY2021**	**FY2017**
	33%	25%
Strongly agree	37%	34%
Agree	12%	18%
Unsure	16%	17%
Disagree	2%	6%
Strongly disagree	100%	100%
Total		

Q2. How confident are you in your employees' ability to detect social engineering lures that could result in a ransomware attack?	**FY2021**	**FY2017**
Very confident	12%	9%
Confident	18%	20%
Somewhat confident	18%	17%
Not confident	52%	54%
Total	100%	100%

Q3a. Do you conduct continuous employee security awareness training?*	**FY2021**	**FY2017**
Yes	61%	55%
No	39%	45%
Total	100%	100%

**wording slightly different in 2017*

Q3b. If yes, does the training cover social engineering, spear phishing and ransomware attacks?	**FY2021**
Yes, full coverage	50%
Yes, some coverage	42%
No coverage	8%
Total	100%

Part 3. Organizational Readiness

Q4a. Using the following 10-point scale, please rate the seriousness with which your organization treats ransomware from 1 = not serious to 10 = extremely serious.	FY2021
1 or 2	14%
3 or 4	12%
5 or 6	19%
7 or 8	20%
9 or 10	35%
Total	100%
Extrapolated value	6.50

Q4b. Using the following 10-point scale, please rate your organization's ability to respond to a ransomware attack from 1 = no ability to 10 = high ability.	FY2021
1 or 2	21%
3 or 4	26%
5 or 6	20%
7 or 8	21%
9 or 10	12%
Total	100%
Extrapolated value	5.04

Q4c. Using the following 10-point scale, please rate your organization's concern about the impact of data leakage related to ransomware attacks from 1 = no concern to 10 = highly concerned.	FY2021
	4%
1 or 2	5%
3 or 4	18%
5 or 6	33%
7 or 8	40%
9 or 10	100%
Total	7.50
Extrapolated value	

Q4d. Using the following 10-point scale, please rate your organization's concern about the risk your supply chain poses to your organization as it relates to ransomware.	FY2021
1 or 2	3%
3 or 4	6%
5 or 6	16%
7 or 8	41%
9 or 10	34%
Total	100%
Extrapolated value	7.44

Q4e. Using the following 10-point scale, please rate how confident your organization is that third parties such as suppliers, cloud providers, and other partners have the necessary privacy and security practices in place to reduce the risk of a data breach involving your organization's sensitive and confidential information.	FY2021
1 or 2	19%
3 or 4	24%
5 or 6	24%
7 or 8	20%
9 or 10	13%
Total	100%
Extrapolated value	5.18

Q5a. Do you evaluate all third parties' security and privacy practices before you engage in a business relationship that requires the sharing of sensitive or confidential information?	FY2021
Yes	36%
Not currently, but plan to in the future	34%
No	30%
Total	100%

Q5b. If yes, how do you perform this evaluation? Please check all that apply.	FY2021
Review written policies and procedures	64%
Acquire signature on contracts that legally obligate the third party to adhere to security and privacy practices	56%
Obtain indemnification from the third party in the event of a data breach	47%
Conduct an assessment of the third party's security and privacy practices	53%
Obtain a self-assessment conducted by the third party	48%
Obtain references from other organizations that engage the third party	36%
Obtain evidence of security certifications	57%
Require completion of a data security questionnaire	51%
Other	5%
Total	417%

Q6. How vulnerable do you feel your organization is to ransomware attacks over the next 12 months?*	FY2021	FY2017
Very vulnerable	31%	30%
Vulnerable	35%	38%
Not very vulnerable	34%	32%
Total	100%	100%

**Scale slightly different in 2021*

Q7. Who in your organization is most responsible for addressing the threat of ransomware?	FY2021	FY2017
Business owner	5%	6%
Senior executive	10%	8%
CIO/CTO	16%	19%
CISO	19%	13%
Backup and disaster recovery team	9%	7%
Incident response team (CSIRT)	6%	5%
Business unit management	5%	9%
Managed security service provider (MSSP)	10%	12%
No one person or function	18%	20%
Other	2%	2%
Total	100%	100%

A ransomware alert is a notice that your system may be targeted or susceptible to a ransomware attack. These alerts are communicated via threat intelligence sharing and law enforcement.

Q8. In the typical week, how many alerts related to ransomware does your organization receive?	FY2021	FY2017
Less than 10	13%	38%
10 to 25	27%	34%
26 to 50	23%	16%
51 to 100	15%	9%
More than 100	7%	3%
Our organization does not have an alert system in place	15%	
Total	100%	100%
Extrapolated value	33.8	24.5

Q9. In your experience, what percentage of these alerts are relevant to your organization?	FY2021	FY2017
Less than 10%	13%	17%
10% to 25%	12%	18%
26% to 50%	40%	36%
51% to 75%	19%	15%
76% to 100%	16%	14%
Total	100%	100%
Extrapolated value	51.40	45.75

Q10. In a typical month, how many attempted attacks do you suspect trigger an alert through one or more security controls but remain undetected? Your best guess is welcome.	FY2021
Less than 1	21%
1 to 5	27%
6 to 10	33%
Greater than 10	19%
Total	100%
Extrapolated value	5.84

Q11. In your opinion, did the pivot to remote work affect the volume and frequency of attacks on your organization?	FY2021
Significant increase	23%
Increase	25%
Stayed the same	30%
Decrease	17%
Significant decrease	5%
Total	100%

Q12. In your opinion, how has the severity of ransomware attacks on your organization changed over the past 12 months?	FY2021	FY2017
Significant increase	25%	18%
Increase	36%	39%
Stayed the same	21%	28%
Decrease	14%	13%
Significant decrease	4%	3%
Total	100%	100%

Part 4. Ransomware experience

Q13. Has your company experienced one or more ransomware attacks?	FY2021	FY2017
Yes, within the past 3 months	30%	18%
Yes, within the past 4 to 6 months	23%	17%
Yes, within the past 7 to 12 months	15%	10%
Yes, more than 12 months ago	12%	6%
No	20%	49%
Total	100%	100%

Q14. How many ransomware incidents do you think your company has experienced in the last 12 months?	FY2021
1 to 2	40%
3 to 5	24%
6 to 10	19%
Greater than 10	17%
Total	100%
Extrapolated value	5.00

Q15. How many ransomware incidents do you think your suppliers have experienced in the last 12 months?	FY2021
1 to 2	39%
3 to 5	25%
6 to 10	19%
Greater than 10	17%
Total	100%
Extrapolated value	5.02

Q16. What type of ransomware did you experience most recently?	FY2021	FY2017
Crypto ransomware	60%	80%
Locker ransomware	21%	20%
Both Crypto and Locker	19%	
Total	100%	100%

Q17. Which extortion tactic did the attackers use to exert pressure?	FY2021
Single (encryption)	31%
Double (data exfiltration)	27%
Triple (DDoS)	25%
Quadruple (communication with stakeholders/customers)	17%
Total	100%

Q18. How was the ransomware unleashed?	FY2021
RDP compromise	34%
Phishing	48%
Software vulnerability	16%
Other (please specify)	2%
Total	100%

Q19. What type of device(s) was compromised by ransomware? Please select all that apply.	FY2021	FY2017
Desktop/laptop	47%	55%
Mobile device	15%	9%
Server	35%	33%
Other	3%	2%
Total	100%	100%

Q20. [If you selected desktop/laptop or mobile device] Was the compromised device used for both personal and business purposes (a.k.a. BYOD/BYOIT)?	FY2021	FY2017
Yes	52%	56%
No	48%	44%
Total	100%	100%

Q21. Did the compromised device infect other devices in the network (e.g., lateral infection)?	FY2021	FY2017
Yes	52%	42%
No	48%	58%
Total	100%	100%

Q22. Which techniques were used for lateral movement and privilege escalation? Please select all that apply.	FY2021
Local administrator weaknesses	39%
Cached credential attacks (mimikatz, etc.)	42%
Weak passwords on high privileged accounts such as service and administrative accounts	45%
Missing patches	33%
Other	2%
Total	161%

Q23. Did the compromised device infect data stored in the cloud?	FY2021	FY2017
Yes	25%	21%
No	75%	79%
Total	100%	100%

Q24. Was sensitive data exfiltrated during the attack?	FY2021
Yes	41%
No	45%
Not sure	14%
Total	100%

Q25a. How much in Bitcoin or other currency was demanded?	FY2021
Less than $25,000	14%
$25,000- $49,000	8%
$50,000- $100,000	9%
$100,000 to $250,000	12%
$250,001 to $500,000	18%
$500,001 to $1,000,000	13%
$1,000,001 to $2,000,000	12%
$2,000,001 to $5,000,000	8%
More than $5,000,000	6%
Total	100%
Extrapolated value	$ 1,017,460

Q25b. In what form was payment demanded?	FY2021
Bitcoin	45%
Other virtual currency	24%
Wired funds	12%
Prepaid cash voucher	10%
Gift cards	6%
Other	3%
Total	100%

Q26a. Did the threat actor impose a time limit for payment?	FY2021	FY2017
Yes, less than 2 days	45%	46%
Yes, 2 to 5 days	30%	28%
Yes, more than 5 days	10%	11%
No	15%	16%
Total	100%	100%

Q26b. If yes, did the threat actor threaten to increase the ransom if the deadline was missed?	FY2021
Yes	54%
No	46%
Total	100%

Q27. Did your company pay the ransom?	FY2021	FY2017
Yes	53%	48%
No	47%	52%
Total	100%	100%

Q28a. If you did not pay a ransom, why not?	FY2021	FY2017
Effective backup strategy	39%	42%
Company policy	15%	16%
Law enforcement advice	11%	10%
Lack of trust in the provision of decryption key	15%	15%
Compromised data wasn't critical	18%	14%
Other	2%	3%
Total	100%	100%

Q28b. What percentage of impacted data were you able to recover?	FY2021
Less than 25%	21%
25 to 50%	30%
50 to 75%	12%
More than 75%	17%
All of the impacted data	20%
Total	100%

Q29a. If you paid the ransom, why did you do so?	FY2021
We have cyber insurance	33%
We cannot afford downtime	34%
We didn’t want our data leaked	23%
Other	10%
Total	100%

Q29b. If you paid, did the cybercriminals provide a decryption key?	FY2021	FY2017
Yes	50%	55%
No	50%	45%
Total	100%	100%

Q30a. Did you report the ransomware incident to law enforcement?	FY2021	FY2017
Yes	43%	49%
No	57%	51%
Total	100%	100%

Q30b. If not, why?	FY2021	FY2017
Did not want to publicize the incident	49%	51%
We were up against a payment deadline	10%	
Did not feel the extortion was exorbitant	14%	17%
Fear of retaliation	9%	10%
Other	18%	21%
Total	100%	100%

Q31. How many people from your organization and/or a third party were involved in the detection, escalation, containment, and remediation of the attack?	FY2021
Less than 5	19%
5 to 10	13%
11 to 15	34%
16 to 20	17%
21 to 30	12%
More than 30	5%
Total	100%
Extrapolated value	13.6

Q32. What were the consequences of the ransomware attack? Please select all that apply.	FY2021	FY2017
We had to shut down for a period	45%	
We lost customers	40%	32%
We had to eliminate jobs	34%	
We lost significant revenue	22%	32%
Our brand was damaged	21%	24%
We had to invest in new security technologies	30%	33%
Other	4%	3%
Total	196%	124%

Part 5. Ransomware Attack Readiness

Q33. Do you think having a full and accurate backup is a sufficient defense against ransomware?

	FY2021
	45%
Yes, backups are sufficient if done right	55%
No, backups alone aren't enough	100%
Total	

Q34. Does your organization regularly engage in security assessments designed to test the ability to prevent and recover from ransomware attacks?

	FY2021
Yes	51%
No	49%
Total	100%

Q35a. Does your organization have a cyber insurance policy that covers ransomware attacks?

	FY2021
Yes	36%
No	64%
Total	100%

Q35b. What is your annual cyber insurance premium?

	FY2021
Less than $5,000	25%
$5,000 to $10,000	27%
$10,001 to $20,000	23%
$20,001 to $50,000	16%
More than $50,000	9%
Total	100%
Extrapolated value	$ 17,100

Q35c. Has your organization's cyber insurance provider modified its ransomware protection over the past year resulting in decreased coverage?

	FY2021
Yes	40%
No	60%
Total	100%

Part 6. Budget

Q36. Approximately, what range best defines your organization's expected 2022 IT security budget?	FY2021
< $1 million	8%
$1 to 5 million	29%
$6 to $10 million	37%
$11 to $50 million	11%
$51 to $100 million	9%
$101 to $250 million	6%
$251 to $500 million	0%
$501 to $750 million	0%
$751 million to $1 billion	0%
More than $1 billion	0%
Total	100%
Extrapolated value	$ 24.42

Q37. Approximately what percentage of the total IT security budget will be allocated to staff and technologies meant to prevent, detect, contain and resolve ransomware attacks?	FY2021
< 10%	19%
10% to 20%	32%
21% to 30%	24%
31% to 40%	9%
41% to 50%	7%
51% to 60%	5%
61% to 70%	1%
71%to 80%	2%
81% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	25%

Part 7. Cost Exposure Estimation

Q38. Following are six cost categories caused by a ransomware attack. Please rank each category based on the financial impact to your organization. 1 = most significant financial impact and 6 = least significant financial impact.	FY2021	Average Rank
Cost of technical support, including forensics and investigative operations	3.34	4
Cost of users' idle time and lost productivity because of IT security failure	2.25	2
Cost resulting from the organization's response to information misuse or theft	2.36	3
Cost associated with legal and regulatory actions	1.65	1
Revenues or income lost because of IT security failure	4.58	6
Cost associated with reputation and brand damage because of IT security failure	3.89	5

Part 8. Organizational Characteristics

D1. What organizational level best describes your current position?	FY2021	FY2017
Business owner	10%	12%
Executive/VP	8%	9%
Director	21%	19%
Manager	19%	17%
Supervisor	16%	1%
Technician	9%	8%
Staff	12%	11%
Consultant	3%	2%
Contractor	2%	2%
Other	0%	1%
Total	100%	100%

D2. Who do you report to within the organization?	FY2021	FY2017
Board of Directors	3%	
CEO/Business Owner	20%	22%
Chief Financial Officer	7%	8%
General Counsel	5%	3%
Chief Information Officer	29%	37%
Chief Information Security Officer	21%	18%
Compliance Officer	3%	2%
Human Resources VP	0%	1%
Chief Security Officer	5%	4%
Data Center Management	0%	4%
Chief Risk Officer	0%	1%
No one, I am the boss	5%	
Other	2%	1%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	FY2021	FY2017
Agriculture & food services	0%	2%
Airlines	0%	0%
Automotive	0%	0%
Communications	3%	2%
Consumer products	6%	7%
E-commerce	6%	0%
Education & research	4%	5%
Energy & utilities	5%	5%
Entertainment & media	4%	5%
Financial services	15%	14%
Health & pharmaceuticals	8%	10%
Hospitality	3%	4%
Industrial	9%	8%
Public sector	8%	6%
Professional services	0%	0%
Retail	9%	8%
Services	8%	10%
Technology & software	8%	8%
Transportation	4%	4%
Other	0%	2%
Total	100%	100%

D4. What is the worldwide headcount of your organization?	FY2021
Less than 200	12%
200 to 500	15%
501 to 1,000	15%
1,001 to 3,000	20%
3,001 to 5,000	16%
5,001 to 8,000	9%
8,001 to 10,000	8%
More than 10,000	5%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.