The Rise of Ransomware

Sponsored by Carbonite

Independently conducted by Ponemon Institute LLC

Publication Date: January 2017

The Rise of Ransomware

Ponemon Institute, January 2017

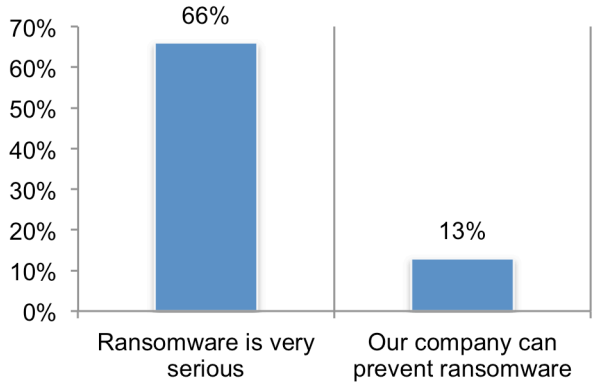
Part 1. Introduction

We are pleased to present the findings of *The Rise of Ransomware*, sponsored by Carbonite, a report on how organizations are preparing for and dealing with ransomware infections.[1] As of September 2016, the Justice Department reported there have been 4,000 ransomware attacks since January 1, 2016. This is a quadrupling of such attacks in just a year.[2]

We surveyed 618 individuals in small to medium-sized organizations who have responsibility for containing ransomware infections within their organization. These individuals, as revealed in this study, dread a ransomware infection and many of them (59 percent of respondents) would rather go without WiFi for a week than deal with a ransomware attack. Furthermore, 77 percent of respondents believe that those who unleash ransomware should pay for the crime. Specifically, 47 percent of respondents say criminals should face criminal prosecution and 27 percent of respondents say they should be subject to civil prosecution.

As shown in Figure 1, there is a significant gap between the perceptions of the seriousness of the threat and the ability of a company to prevent ransomware in the future. While 66 percent of respondents rate the threat of ransomware as very serious, only 13 percent of respondents rate their companies' preparedness to prevent ransomware as high.

Figure 1. The ransomware prevention gap
1 = low to 10 = high, 7+ responses reported



Fifty-one percent of companies represented in this research have experienced a ransomware attack. The following explains how these companies were affected.

- Companies experienced an average of 4 ransomware attacks and paid an average of $2,500 per attack.
- If companies didn't pay ransom, it was because they had a full and accurate backup. Respondents also believe a full and accurate backup is the best defense.
- Companies suffered financial consequences such as the need to invest in new technologies, the loss of customers and lost money due to downtime.
- Cyber criminals were most likely to use phishing/social engineering and insecure websites to unleash ransomware. Respondents believe the cyber criminal specifically targeted their company.
- Compromised devices infected other devices in the network. Very often, data was exfiltrated from the device.
- Companies were reluctant to report the incident to law enforcement because of concerns about negative publicity.

---

[1] Ransomware is a sophisticated piece of malware that blocks the victim's access to his/her files. While there are many strains of ransomware today, the two prominent types are; encrypting ransomware and locker ransomware.

[2] "FBI Official Explains What to Do in a Ransomware Attack," by Steve Zurier, Dark Reading, September 7, 2016.

Following are the key takeaways from this research.

Many companies think they are too small to be a target. Perceptions about the likelihood of an infection affect ransomware prevention and detection procedures. Fifty-seven percent of respondents believe their company is too small to be a target of ransomware and, as a result, only 46 percent of respondents believe prevention of ransomware attacks is a high priority for their company. Despite not being a high priority, 59 percent of respondents believe a ransomware attack would have serious financial consequences for their company and 53 percent of respondents would consider paying a ransom if their company's data was lost (100 percent – 47 percent of respondents who would never pay a ransom).

Current technologies are not considered sufficient to prevent ransomware infections. Only 27 percent of respondents are confident their current antivirus software will protect their company from ransomware. There is also concern about how the use of Internet of Things connected devices will increase their risk of ransomware.

Inability to detect all ransomware infections puts companies at risk. An average of one or more ransomware infections go undetected per month and are able to bypass their organization's IPS and/or AV systems, according to 44 percent of respondents. However, 29 percent of respondents say they cannot determine how many ransomware infections go undetected in a typical month.

One or more ransomware attacks are believed to be possible in the next 12 months. Sixty-eight percent of respondents believe their company is very vulnerable (30 percent) or vulnerable (38 percent) to a ransomware attack. Relative to other types of cyber attacks, 67 percent of respondents say ransomware is much worse (35 percent) or worse (32 percent).

The severity and volume of ransomware infections have increased over the past 12 months. Sixty percent of respondents say the volume or frequency of ransomware infections have significantly increased (22 percent) or increased (38 percent). Fifty-seven percent say the severity of ransomware infections have significantly increased (18 percent) or increased (39 percent) over the past 12 months. In a typical week, the companies documented in this research have experienced an average of 26 ransomware alerts per week. An average of 47 percent of these alerts are considered reliable.

Negligent and uninformed employees put companies at risk. Fifty-eight percent of respondents say negligent employees put their company at risk for a ransomware attack. Only 29 percent of respondents are very confident (9 percent) or confident (20 percent) their employees can detect risky links or sites that could result in a ransomware attack.

To prevent ransomware infections, employees need to become educated on the ransomware threat. Fifty-five percent of respondents say their organizations conduct training programs on what employees should be doing to protect data. However, only 33 percent of respondents say their companies address the ransomware threat.

Most companies experience encrypting ransomware. Fifty-one percent of respondents had a ransomware incident within the past 3 months to more than one year ago**.** Eighty percent of respondents say they experienced encrypting ransomware and 20 percent of respondents say their company experienced locker ransomware. These companies have experienced an average of 4 ransomware incidents. Most respondents (59 percent) believe the cyber criminal specifically targeted them and their company.

The consequences of ransomware are costly. The top consequences of a ransomware attack are financial. Attacks required companies to invest in new security technologies (33 percent of respondents), customers were lost (32 percent of respondents) and lost money due to downtime

(32 percent of respondents). Moreover, the ransomware incident is believed to make their company more vulnerable to future attacks (49 percent of respondents).

By far, most ransomware incidents are unleashed as a result of phishing and insecure websites. Forty-three percent of respondents say the ransomware was unleashed by phishing/social engineering and 30 percent of respondents say it was unleashed by insecure or spoofed websites. Desktops/laptops and servers were the devices most often compromised at 55 percent and 33 percent of respondents, respectively.

According to 56 percent of respondents, the compromised device was used for both personal and business purposes. The compromised device infected other devices in the network (42 percent of respondents) and the cloud (21 percent of respondents).

Many companies paid the ransom. Forty-eight percent of respondents say their company paid the ransom. The average payment was $2,500. A key element in making ransomware work for the attacker is a convenient payment system that is hard to trace. The ransom was most often paid using Bitcoin (33 percent of respondents) or cash (25 percent of respondents). Fifty-five percent of respondents say once the payment was made, the cyber criminal provided the decryption cypher or key to unlock compromised devices.

Attackers demand speedy payment. Forty-six percent of respondents say the attacker wanted payment in less than two days. Only 16 percent did not place a time limit for payment.

Data was exfiltrated from the compromised device. Fifty-five percent of respondents say with certainty or it was likely that the ransomware exfiltrated data from the compromised device(s). On average companies spent 42 hours dealing with and containing the ransomware incident.

Full and accurate backup is a critical ransomware defense. Fifty-two percent of respondents did not pay the ransom because they had full backup (42 percent of respondents). Sixty-eight percent of respondents in companies that experienced a ransomware incident say it is essential (30 percent) or very important (38 percent) to have a full and accurate backup as a defense against future ransomware incidents.

Fear of publicity stops companies from reporting the incident to law enforcement. Despite the FBI's pleas to report the incident to law enforcement, 49 percent of respondents say their company did not report the ransomware attack. As shown in Figure 16, the primary reason was to avoid the publicity.

Part 2. 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.

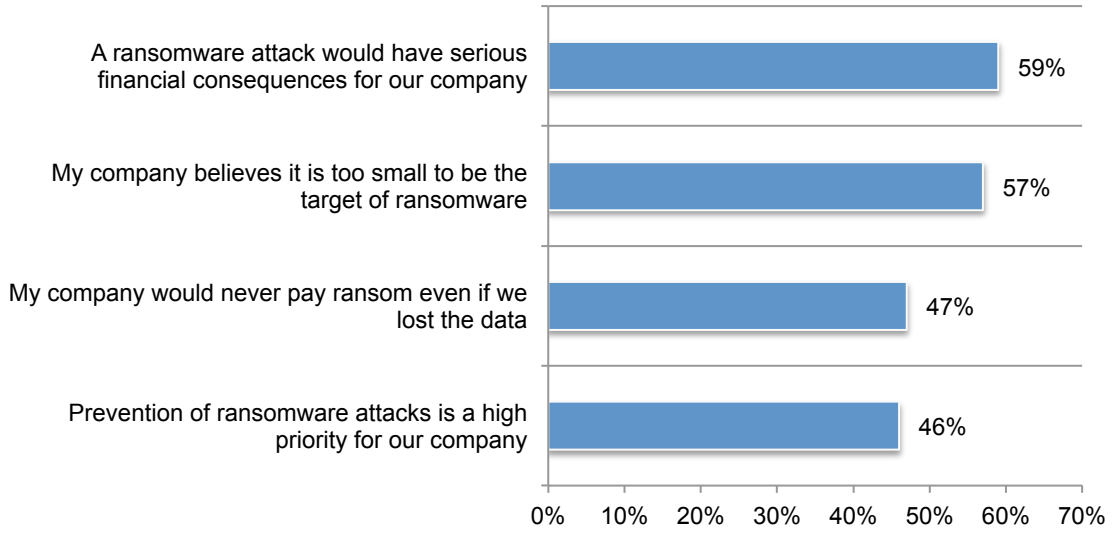
- Ransomware threat response readiness
- Employees are the weakest link in the defense against ransomware
- The consequences of a ransomware infection: the experiences of targeted companies

Ransomware threat response readiness

Many companies think they are too small to be a target. Perceptions about the likelihood of an infection affect ransomware prevention and detection procedures.

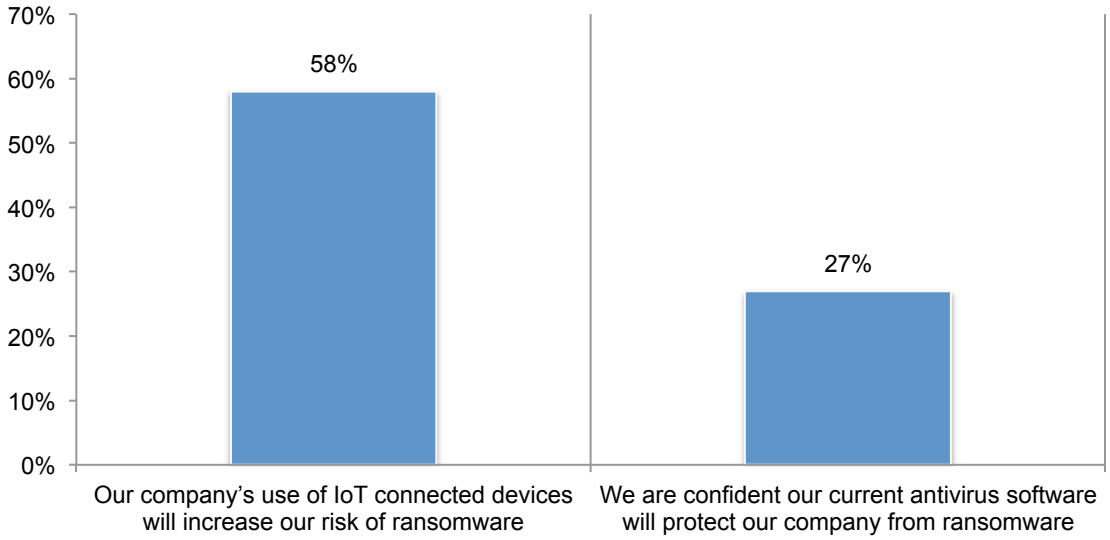
As shown in Figure 2, 57 percent of respondents believe their company is too small to be a target of ransomware and, as a result, only 46 percent of respondents believe prevention of ransomware attacks is a high priority for their company. Despite not being a high priority, 59 percent of respondents believe a ransomware attack would have serious financial consequences for their company and 53 percent of respondents would consider paying ransom if their company's data was lost (100 percent – 47 percent of respondents who would never pay a ransom).

Figure 2. Perceptions about ransomware
Strongly agree and Agree responses combined



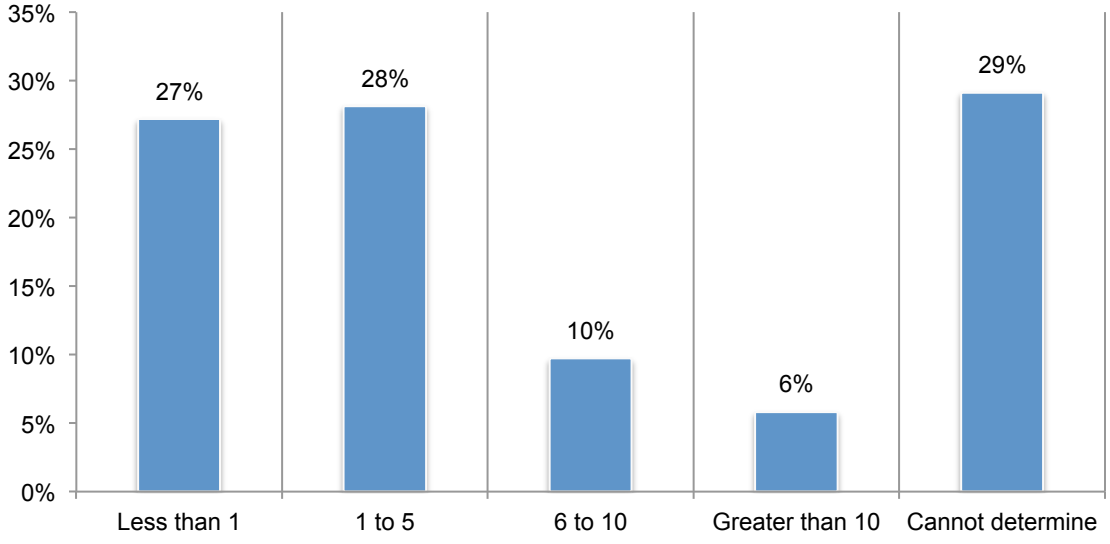
Current technologies are not considered sufficient to prevent ransomware infections. According to Figure 3, only 27 percent of respondents are confident their current antivirus software will protect their company from ransomware. There is also concern about how the use of Internet of Things connected devices will increase their risk of ransomware.

Figure 3. The difficulty in dealing with the risk of ransomware
Strongly agree and Agree responses combined



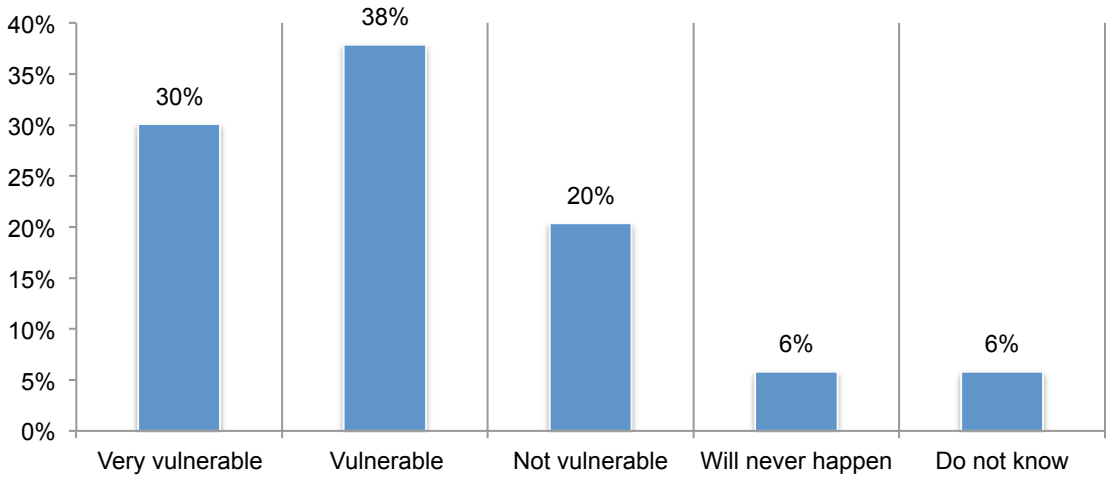
Inability to detect all ransomware infections puts companies at risk. As shown in Figure 4, an average of 1 or more ransomware infections go undetected per month and are able to bypass their organization's IPS and/or AV systems, according to 44 percent of respondents. However, 29 percent of respondents say they cannot determine how many ransomware infections go undetected in a typical month.

Figure 4. In a typical month, how may ransomware infections go undetected?



One or more ransomware attacks are believed to be possible in the next 12 months. Sixty-eight percent of respondents, as shown in Figure 5, believe their company is very vulnerable (30 percent) or vulnerable (38 percent) to a ransomware attack. Relative to other types of cyber attacks, 67 percent of respondents say ransomware is much worse (35 percent) or worse (32 percent).

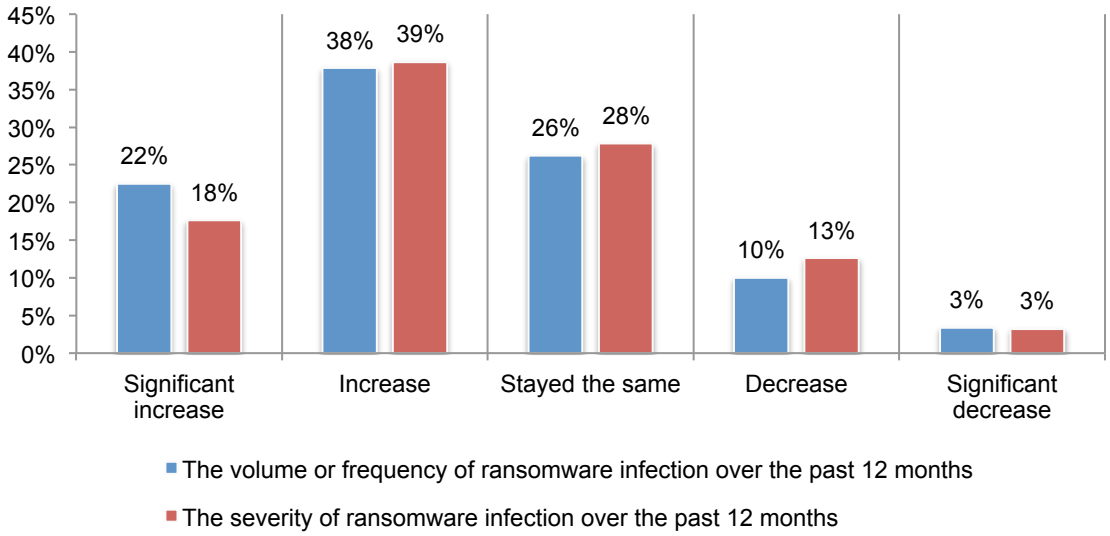
Figure 5. How vulnerable do you feel your company is to a ransomware attack over the next 12 months?



The severity and volume of ransomware infections have increased over the past 12 months. According to Figure 6, 60 percent of respondents say the volume or frequency of ransomware infections have significantly increased (22 percent) or increased (38 percent). Fifty-seven percent say the severity of ransomware infections have significantly increased (18 percent) or increased (39 percent) over the past 12 months.

In a typical week, companies in this research have experienced an average of 26 ransomware alerts per week. An average of 47 percent of these alerts are considered reliable.

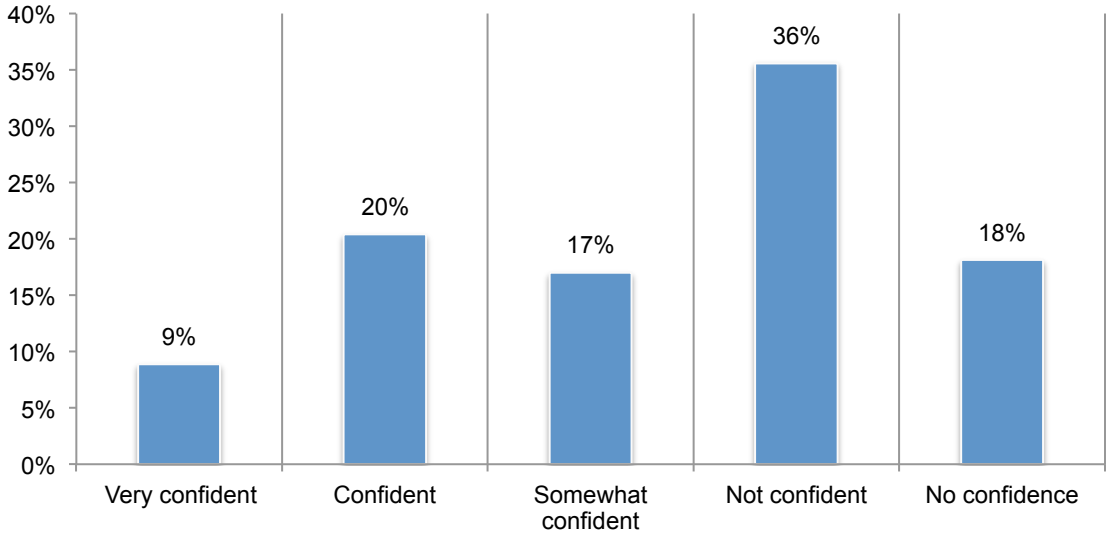
Figure 6. How has the volume and severity of ransomware infections changed over the past 12 months?



Employees are the weakest link in the defense against ransomware

Negligent and uninformed employees put companies at risk. Fifty-eight percent of respondents say negligent employees put their company at risk for a ransomware attack. As shown in Figure 7, only 29 percent of respondents are very confident (9 percent) or confident (20 percent) their employees can detect risky links or sites that could result in a ransomware attack.

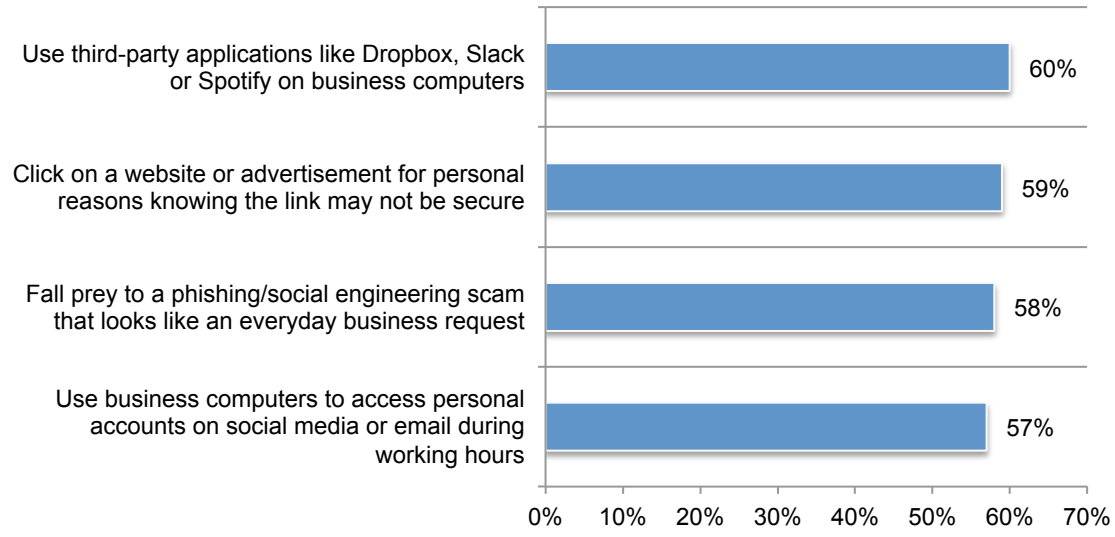
Figure 7. How confident are you that your employees can detect risky links or sites that could result in a ransomware attack?



To prevent ransomware, employees' risky behaviors should be stopped. Figure 8 reveals the risky employee behaviors most respondents believe are occurring in their companies. These include: clicking on a website or advertisement for personal reasons (e.g., fitness or shopping site), knowing the link may not be secure (59 percent of respondents), using business computers to access personal accounts on social media or email during working hours (57 percent of respondents), falling prey to a phishing/social engineering scam that looks like an everyday business request (58 percent of respondents) or using third-party applications like Dropbox, Slack or Spotify on business computers (60 percent of respondents).

To prevent ransomware infections, employees need to become educated on the ransomware threat. Fifty-five percent of respondents say their organizations conduct training programs on what employees should be doing to protect data. However, only 33 percent of respondents say their companies address the ransomware threat.

Figure 8. How employees put companies at risk for a ransomware infection
Very likely and Likely responses combined



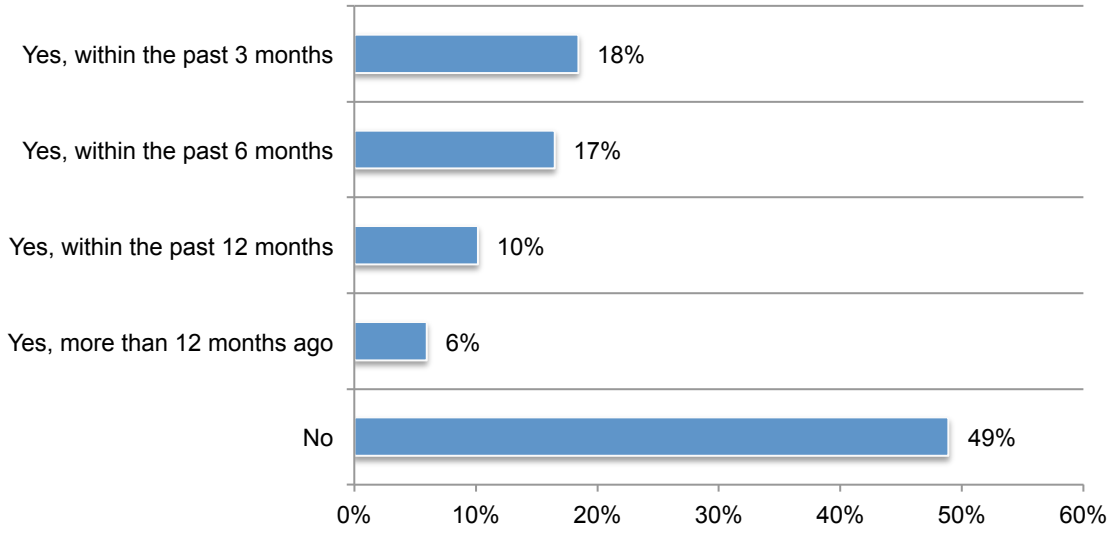
The consequences of a ransomware infection: the experiences of targeted companies

The following findings are based on the 51 percent of respondents who say that their companies experienced ransomware.

Most companies experience encrypting ransomware.[3] As shown in Figure 9, 51 percent of respondents had a ransomware incident within the past 3 months to more than one year ago.

Eighty percent of respondents say this is the type of ransomware they experienced and 20 percent of respondents say their company experienced locker ransomware. These companies have experienced an average of 4 ransomware incidents. Most respondents (59 percent) believe the cyber criminal specifically targeted them and their company.

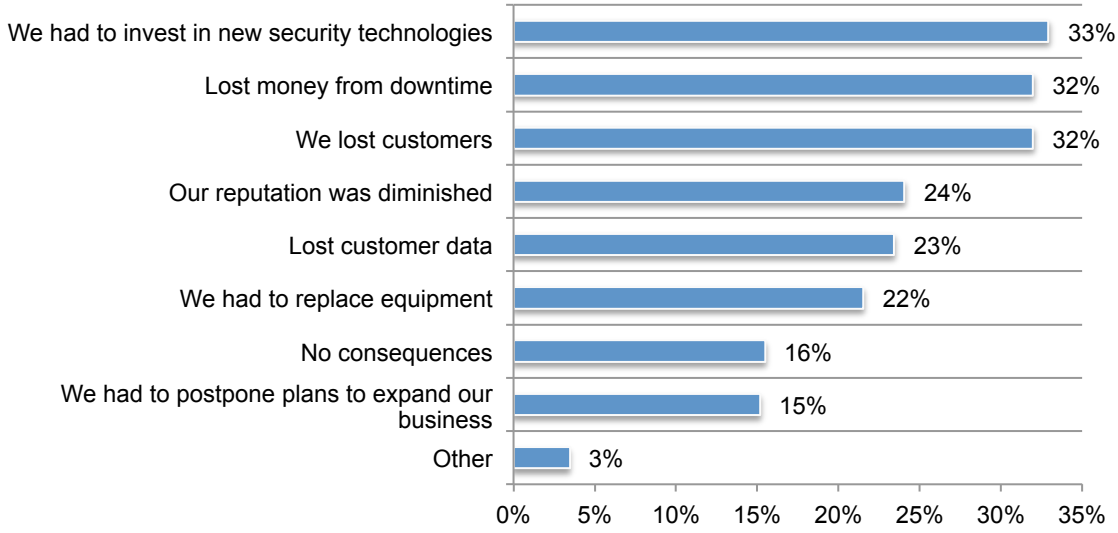
Figure 9. Have you or your company experienced ransomware?



[3] 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.

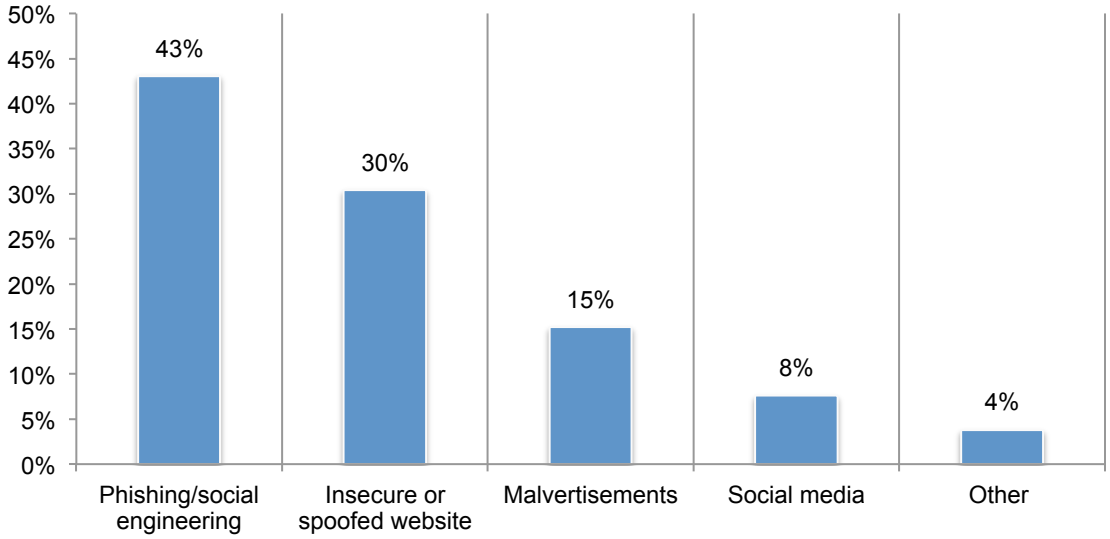
The consequences of ransomware are costly. The top consequences of a ransomware attack are financial, as shown in Figure 10. The attacks required companies to invest in new security technologies (33 percent of respondents), customers were lost (32 percent of respondents) and lost money due to downtime (32 percent of respondents). Moreover, the ransomware incident is believed to make their company more vulnerable to future attacks (49 percent of respondents).

Figure 10. What were the consequences of the ransomware attack?
Two choices permitted



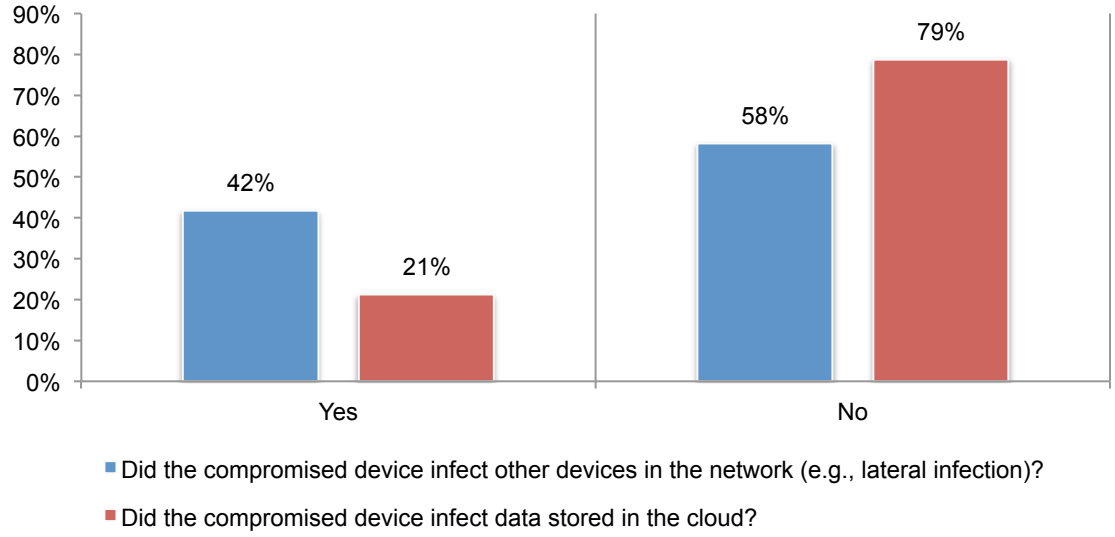
By far, most ransomware incidents are unleashed as a result of phishing and insecure websites. According to Figure 11, 43 percent of respondents say the ransomware was unleashed by phishing/social engineering and 30 percent of respondents say it was unleashed by insecure or spoofed websites. Desktop/laptops and servers were the devices most often compromised, at 55 percent and 33 percent of respondents, respectively.

Figure 11. How was the ransomware unleashed?



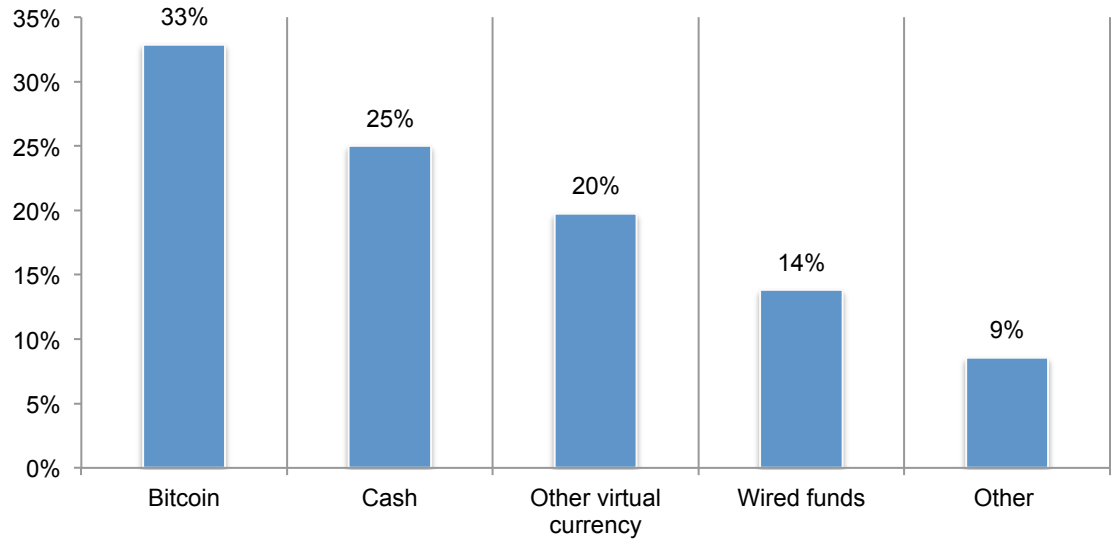
According to 56 percent of respondents, the compromised device was used for both personal and business purposes. As shown in Figure 12, the compromised device infected other devices in the network (42 percent of respondents) and the cloud (21 percent of respondents).

Figure 12. Did the compromised device infect other devices in the network and data stored in the cloud?



Many companies paid the ransom. Forty-eight percent of respondents say their company paid the ransom. The average payment was $2,500. A key element in making ransomware work for the attacker is a convenient payment system that is hard to trace.[4] As shown in Figure 13, the ransom was most often paid using Bitcoin (33 percent of respondents) or cash (25 percent of respondents). Fifty-five percent of respondents say that once the payment was made, the cyber criminal provided the decryption cypher or key to unlock the compromised devices.

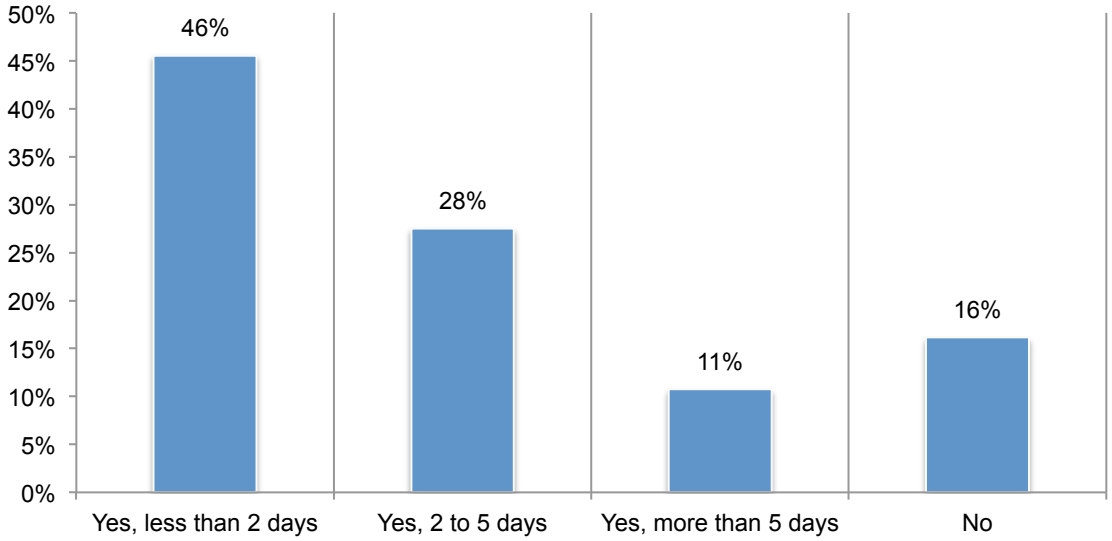
Figure 13. How did your company pay the ransom?



[4] See Wikipedia

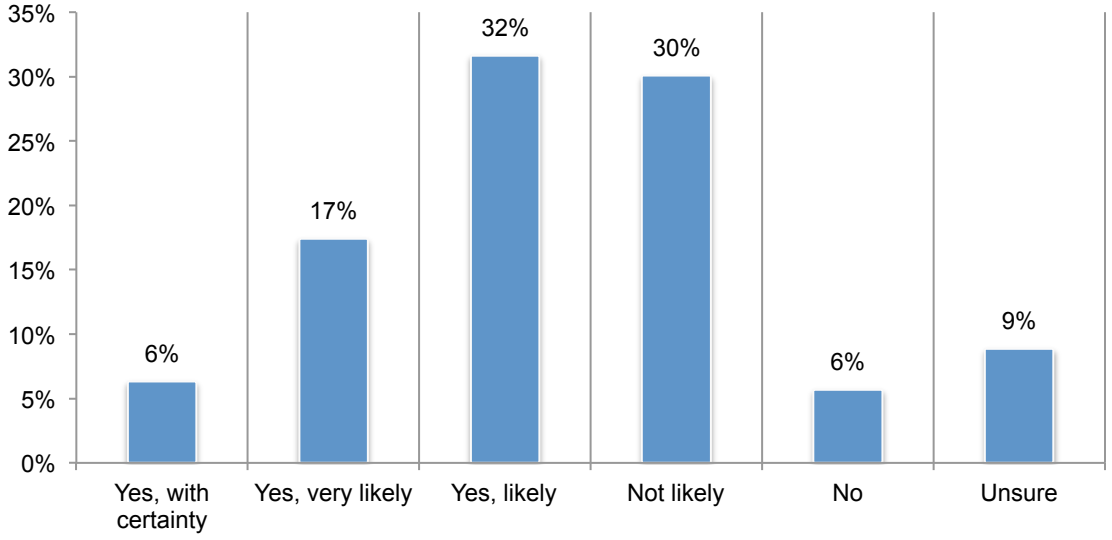
Attackers demand speedy payment. As shown in Figure 14, 46 percent of attackers wanted payment in less than two days. Only 16 percent did not place a time limit for payment.

Figure 14. Did the ransomware place a time limit for payment?



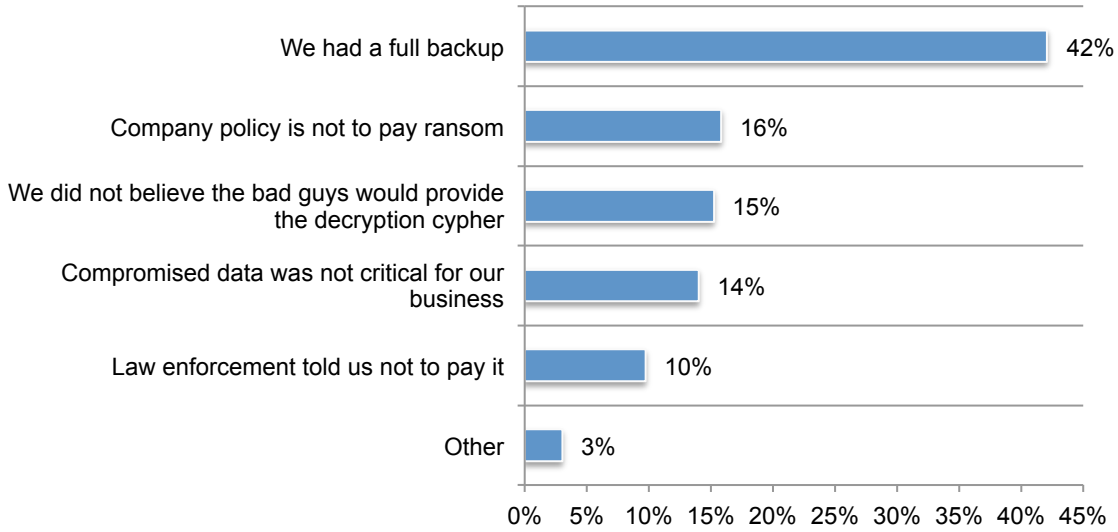
Data was exfiltrated from the compromised device. According to Figure 15, 55 percent of respondents say with certainty or it was likely that the ransomware exfiltrated data from the compromised device(s). On average companies spent 42 hours dealing with and containing the ransomware incident.

Figure 15. Did the ransomware exfiltrate data from the compromised device(s)?



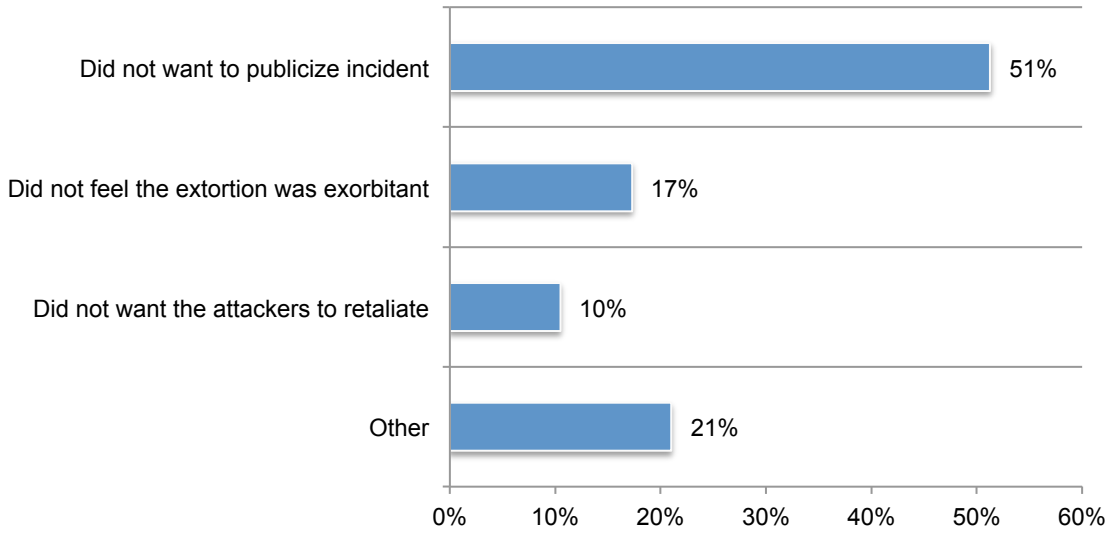
Full and accurate backup is a critical ransomware defense. Fifty-two percent of respondents did not pay the ransom because they had a full backup (42 percent of respondents), as shown in Figure 16. Sixty-eight percent of respondents in companies that experienced a ransomware incident say it is essential (30 percent) or very important (38 percent) to have a full and accurate backup as a defense against future ransomware incidents.

Figure 16. Why was ransom not paid?



Fear of publicity stops companies from reporting the incident to law enforcement. The FBI is urging businesses or consumers hit by ransomware to refuse to pay the ransom and immediately contact the FBI or file a complaint. "Whether it's a Bitcoin wallet address, transaction data, the hashtag of the malware, or any email correspondence, it can help advance an FBI ransomware investigation," said Will Bales, supervisory special agent for the FBI's Cyber Division.[5] Despite the FBI's pleas, 49 percent of respondents say their company did not report the ransomware attack. As shown in Figure 17, the primary reason was to avoid the publicity.

Figure 17. Why did your company not report the incident to law enforcement?



[5] Ibid, Dark Reading

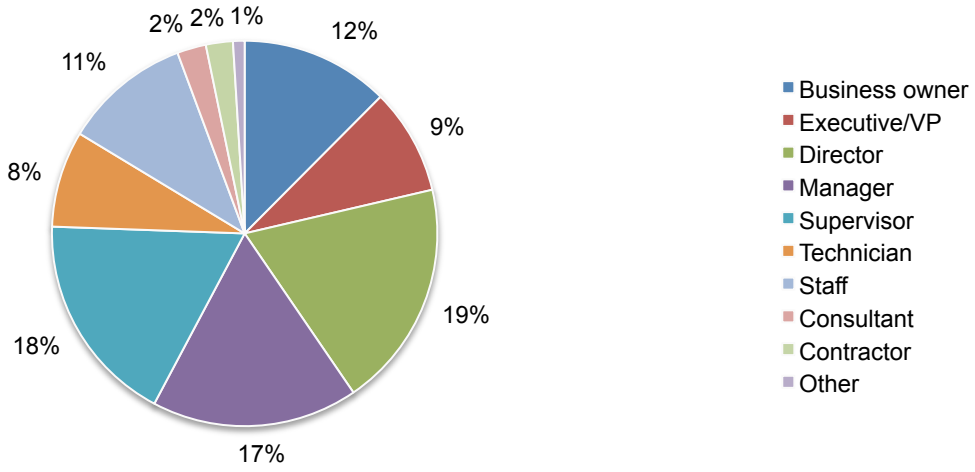
Part 3. Methods

A sampling frame composed of 15,580 individuals who have responsibility for containing ransomware infections within the organization were selected for participation in this survey. As shown in Table 1, 685 respondents completed the survey. Screening removed 67 respondent surveys. The final sample was 618 respondent surveys (or a 4.0 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	15,580	100.0%
Total returns	685	4.4%
Rejected surveys	67	0.4%
Final sample	618	4.0%

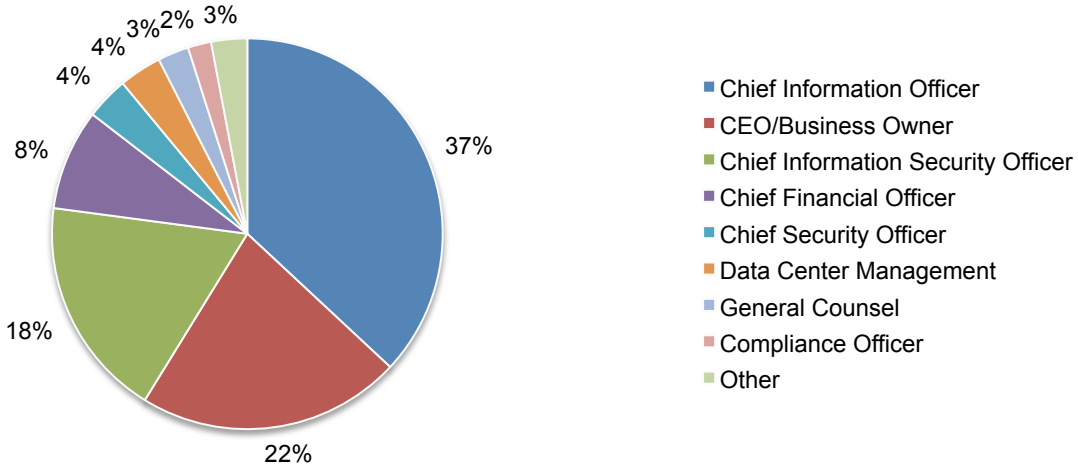
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (75 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



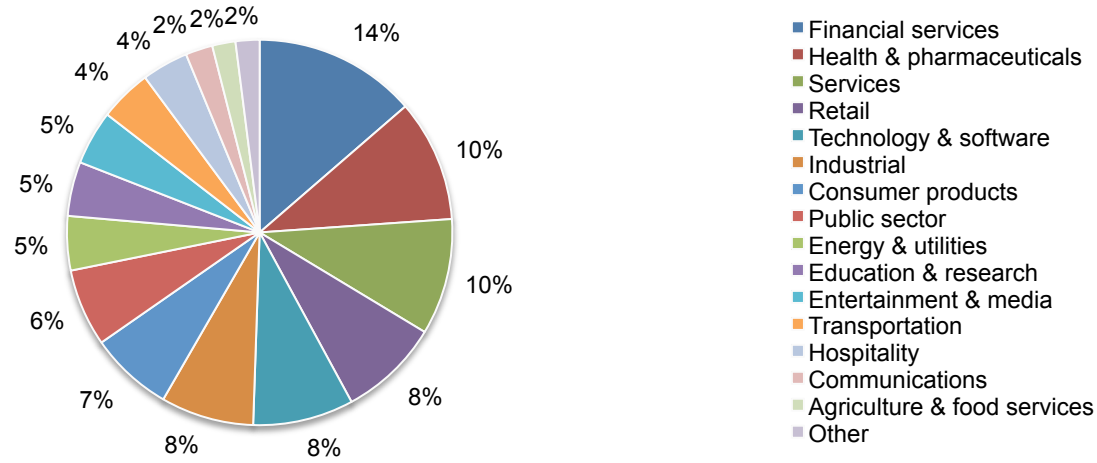
As shown in Pie Chart 2, 37 percent of respondents report directly to the CIO, 22 percent report to the CEO/business owner and 18 percent report to the CISO.

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



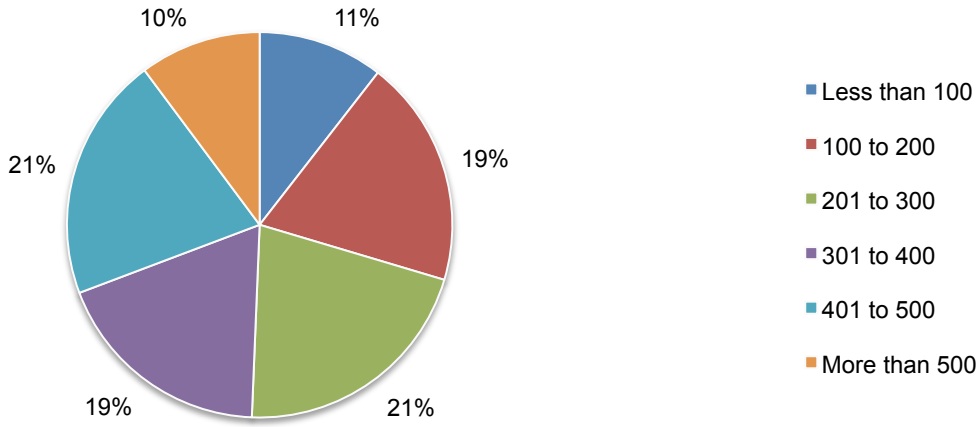
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (14 percent of respondents) as the largest segment, followed by health and pharmaceuticals (10 percent of respondents) and services (10 percent of respondents).

Pie Chart 3. Primary industry focus



According to Pie Chart 4, 50 percent of the respondents are from organizations with a global headcount of more than 300 employees.

Pie Chart 4. Worldwide headcount of the organization



Part 4. 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.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in September 2016.

Survey response	Freq	Pct%
Total sampling frame	15,580	100.0%
Total returns	685	4.4%
Rejected surveys	67	0.4%
Final sample	618	4.0%

Part 1. Screening questions

S1. How familiar are you with ransomware?	Pct%
Very familiar	28%
Familiar	55%
Somewhat familiar	17%
No knowledge (Stop)	0%
Total	100%

S2. Do you have any responsibility in containing ransomware infections within your organization?	Pct%
Yes, full responsibility	33%
Yes, some responsibility	50%
Yes, minimum responsibility	18%
No responsibility (Stop)	0%
Total	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.	Pct%
Strongly agree	22%
Agree	35%
Unsure	21%
Disagree	16%
Strongly disagree	6%
Total	100%

Q1b. My company would never pay ransom even if we lost the data.	Pct%
Strongly agree	19%
Agree	28%
Unsure	21%
Disagree	22%
Strongly disagree	10%
Total	100%

Q1c. Negligent employees put our company at risk for a ransomware attack.	Pct%
Strongly agree	23%
Agree	35%
Unsure	17%
Disagree	19%
Strongly disagree	6%
Total	100%

Q1d. A ransomware attack would have serious financial consequences for our company.	Pct%
Strongly agree	25%
Agree	34%
Unsure	18%
Disagree	17%
Strongly disagree	6%
Total	100%

Q1e. Prevention of ransomware attacks is a high priority for our company.	Pct%
Strongly agree	18%
Agree	28%
Unsure	22%
Disagree	20%
Strongly disagree	12%
Total	100%

Q1f. I would rather go without WiFi for a week than deal with a ransomware attack.	Pct%
Strongly agree	25%
Agree	34%
Unsure	17%
Disagree	18%
Strongly disagree	6%
Total	100%

Q1g. Our company's use of IoT connected devices will increase our risk of ransomware.	Pct%
Strongly agree	22%
Agree	36%
Unsure	18%
Disagree	17%
Strongly disagree	6%
Total	100%

Q1h. We are confident our current antivirus software will protect our company from ransomware.	Pct%
Strongly agree	9%
Agree	18%
Unsure	26%
Disagree	32%
Strongly disagree	15%
Total	100%

Q2. How confident are you that your employees can detect risky links or sites that could result in a ransomware attack?	Pct%
Very confident	9%
Confident	20%
Somewhat confident	17%
Not confident	36%
No confidence	18%
Total	100%

Q3. How likely would your employees do the following?	
Q3a. Click on a website or advertisement for personal reasons (e.g. fitness or shopping site) knowing the link may not be secure	Pct%
Very likely	23%
Likely	36%
Not likely	23%
Never	15%
Unsure	3%
Total	100%

Q3b. Use business computers to access personal accounts on social media or email during working hours	Pct%
Very likely	22%
Likely	35%
Not likely	24%
Never	15%
Unsure	3%
Total	100%

Q3c. Fall prey to a phishing/social engineering scam that looks like an everyday business request	Pct%
Very likely	24%
Likely	34%
Not likely	22%
Never	17%
Unsure	3%
Total	100%

Q3d. Use third-party applications like Dropbox, Slack or Spotify on business computers	Pct%
Very likely	23%
Likely	37%
Not likely	22%
Never	15%
Unsure	3%
Total	100%

Q4a. Do you conduct training programs on what your employees should be doing to protect data?	Pct%
Yes	55%
No	45%
Total	100%

Q4b. If yes, does the training program cover the ransomware threat?	Pct%
Yes	33%
No	67%
Total	100%

Q5. What keeps you up at night? Please check the top two reasons.	Pct%
Cyber attack	30%
Ransomware attack	26%
Lawsuit	11%
Regulatory fine	9%
Bankruptcy	9%
Malicious insider	20%
Loss of a major client	28%
Business disruption	18%
Disruption to IT (downtime)	35%
Other (please specify)	6%
Total	192%

Q6. Which devices do you believe are most vulnerable to a ransomware attack?	Pct%
Desktop/laptop	44%
Mobile device	17%
Server	23%
All of the above are equally vulnerable	17%
Total	100%

Q7. How should those who commit ransomware be punished?	Pct%
Criminal prosecution	47%
Civil prosecution	27%
No prosecution if they cooperate	15%
Unsure	11%
Total	100%

Part 3. Organizational readiness

Q8a. Using the following 10-point scale, please rate how serious is the threat of ransomware.	Pct%
1 or 2	7%
3 or 4	9%
5 or 6	18%
7 or 8	32%
9 or 10	34%
Total	100%
Extrapolated value	7.0

Q8b. Using the following 10-point scale, please rate how prepared is your company to prevent ransomware in the future.	Pct%
1 or 2	31%
3 or 4	33%
5 or 6	23%
7 or 8	9%
9 or 10	4%
Total	100%
Extrapolated value	3.9

Q9. How vulnerable do you feel your company is to one or more ransomware attacks over the next 12 months?	Pct%
Very vulnerable	30%
Vulnerable	38%
Not vulnerable	20%
Will never happen	6%
Do not know	6%
Total	100%

Q10. Relative to other types of cyber attacks, how serious is ransomware?	Pct%
Much worse	35%
Worse	32%
The same	17%
Less worse	11%
Much less worse	5%
Total	100%

Q11. Who in your organization is most responsible for dealing with/containing ransomware?	Pct%
Business owner	6%
Senior executive	8%
CIO/CTO	19%
CISO	13%
Backup and disaster recovery team	7%
Incident response team (CSIRT)	5%
Business unit management	9%
Managed security service provider (MSSP)	12%
No one person or function	20%
Other (please specify)	2%
Total	100%

Q12. In the typical week, how many ransomware alerts does your organization receive?	Pct%
Less than 10	38%
10 to 25	34%
26 to 50	16%
51 to 100	9%
More than 100	3%
Total	100%
Extrapolated value	26.06

Q13. In your experience, what percent of these alerts are reliable?	Pct%
Less than 10%	17%
10% to 25%	18%
26% to 50%	36%
51% to 75%	15%
76% to 100%	14%
Total	100%
Extrapolated value	46.52

Q14. In the typical month, how many ransomware infections go undetected (i.e., they bypass your organization's IPS and/or AV systems)? Your best guess is welcome.	Pct%
Less than 1	27%
1 to 5	28%
6 to 10	10%
Greater than 10	6%
Cannot determine	29%
Total	100%
Extrapolated value	

Q15. In your opinion, how has the volume or frequency of ransomware infection changed over the past 12 months?	Pct%
Significant increase	22%
Increase	38%
Stayed the same	26%
Decrease	10%
Significant decrease	3%
Total	100%

Q16. In your opinion, how has the severity of ransomware infection changed over the past 12 months?	Pct%
Significant increase	18%
Increase	39%
Stayed the same	28%
Decrease	13%
Significant decrease	3%
Total	100%

Part 4. Ransomware experience

Q17. Have you or your company experienced ransomware?	Pct%
Yes, within the past 3 months	18%
Yes, within the past 6 months	17%
Yes, within the past 12 months	10%
Yes, more than 12 months ago	6%
No (Go to D1)	49%
Total	100%

Q18. How many ransomware incidents have you or your company experienced?	Pct%
Less than 1	29%
1 to 5	41%
6 to 10	18%
Greater than 10	12%
Total	100%
Extrapolated value	4.35

Q19. What type of ransomware did you experience?	Pct%
Encrypting ransomware.	80%
Locker ransomware	20%
Total	100%

Q20. How was the ransomware unleashed?	Pct%
Phishing/social engineering	43%
Insecure or spoofed website	30%
Social media	8%
Malvertisements	15%
Other (please specify)	4%
Total	100%

Q21. What type of device was compromised by ransomware?	Pct%
Desktop/laptop	55%
Mobile device	9%
Server	33%
Other (please specify)	2%
Total	100%

Q22. [If you selected desktop/laptop or mobile device] Was the compromised device used for both personal and business purposes (a.k.a. BYOD)?	Pct%
Yes	56%
No	44%
Total	100%

Q23. Did the compromised device infect other devices in the network (e.g., lateral infection)?	Pct%
Yes	42%
No	58%
Total	100%

Q24. Did the compromised device infect data stored in the cloud?	Pct%
Yes	21%
No	79%
Total	100%

Q25. How much was the ransom?	Pct%
Less than $100	10%
$100 to $500	21%
$501 to $1,000	35%
$1,001 to $5,000	16%
$5,001 to $10,000	11%
More than $10,000	7%
Total	100%
Extrapolated value	2,511

Q26. Did the ransomware place a time limit for payment?	Pct%
Yes, less than 2 days	46%
Yes, 2 to 5 days	28%
Yes, more than 5 days	11%
No	16%
Total	100%

Q27a. Did your company pay the ransom?	Pct%
Yes	48%
No	52%
Total	100%

Q27b. If you paid a ransom, how did you do it?	Pct%
Bitcoin	33%
Other virtual currency	20%
Wired funds	14%
Cash	25%
Other (please specify)	9%
Total	100%

Q27c. If you did not pay a ransom, why not?	Pct%
We had a full backup	42%
Company policy is not to pay ransom	16%
Law enforcement told us not to pay it	10%
We did not believe the bad guys would provide the decryption cypher	15%
Compromised data was not critical for our business	14%
Other	3%
Total	100%

Q27d. If you paid, did the cyber criminal provide the decryption cypher or key to unlock compromised devices?	Pct%
Yes	55%
No	45%
Total	100%

Q28a. Did you report the ransomware incident to law enforcement?	Pct%
Yes	49%
No	51%
Total	100%

Q28b. If no, why?	Pct%
Did not want to publicize incident	51%
Did not want the attackers to retaliate	10%
Did not feel the extortion was exorbitant	17%
Other (please specify)	21%
Total	100%

Q29. Did the ransomware exfiltrate (move) data from the compromised device(s)?	Pct%
Yes, with certainty	6%
Yes, very likely	17%
Yes, likely	32%
Not likely	30%
No	6%
Unsure	9%
Total	100%

Q30. Approximately, how many hours was spent to deal with and contain the ransomware incident? Please estimate the aggregate hours of all personnel involved for one ransomware incident.	Pct%
Less than 5	10%
5 to 10	17%
11 to 25	20%
26 to 50	23%
51 to 100	20%
More than 100	11%
Total	100%
Extrapolated value	41.64

Q31. Do you believe the cyber criminal specifically targeted you or your company?	Pct%
Yes	59%
No	41%
Total	100%

Q32. Has the ransomware incident made you or your company more vulnerable to future ransomware attacks?	Pct%
Yes	49%
No	51%
Total	100%

Q33. In your opinion, how important is having a full and accurate backup as a defense against future ransomware incidents?	Pct%
Essential	30%
Very important	38%
Important	21%
Not important	9%
Irrelevant	2%
Total	100%

Q34. What were the consequences of the ransomware attack? Top 2 choices	Pct%
We had to postpone plans to expand our business	15%
We lost customers	32%
Our reputation was diminished	24%
We had to invest in new security technologies	33%
We had to replace equipment	22%
Lost customer data	23%
Lost money from downtime	32%
No consequences	16%
Other	3%
Total	200%

Part 5. Cost exposure estimation

Q35. Please approximate the total potential cost exposure that could result from all IT security failures over the course of one year.	Pct%
Zero	5%
Less than $10,000	3%
$10,001 to $100,000	4%
$100,001 to $250,000	11%
$250,001 to $500,000	13%
$500,001 to $1,000,000	15%
$1,000,001 to $5,000,000	17%
$5,000,001 to $10,000,000	12%
$10,000,001 to $25,000,000	4%
$25,000,001 to $50,000,000	2%
$50,00,001 to $100,000,000	1%
More than $100,000,000	1%
Cannot determine	12%
Total	100%
Extrapolated value	$8,174,383

Part 6. Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Business owner	12%
Executive/VP	9%
Director	19%
Manager	17%
Supervisor	18%
Technician	8%
Staff	11%
Consultant	2%
Contractor	2%
Other	1%
Total	100%

D2. Check the person you report to within the organization.	Pct%
CEO/Business Owner	22%
Chief Financial Officer	8%
General Counsel	3%
Chief Information Officer	37%
Chief Information Security Officer	18%
Compliance Officer	2%
Human Resources VP	1%
Chief Security Officer	4%
Data Center Management	4%
Chief Risk Officer	1%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Financial services	14%
Health & pharmaceuticals	10%
Retail	8%
Services	10%
Public sector	6%
Technology & software	8%
Industrial	8%
Consumer products	7%
Energy & utilities	5%
Hospitality	4%
Transportation	4%
Communications	2%
Education & research	5%
Entertainment & media	5%
Agriculture & food services	2%
Defense & aerospace	1%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 100	11%
100 to 200	19%
201 to 300	21%
301 to 400	19%
401 to 500	21%
More than 500	10%
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 high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict 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.