2017

RANSOMWARE DEFENSE SURVEY

The Enterprise Strikes Back

INSIDE:

- Complete Survey Results
- Expert Analysis
- Insights from Leading Industry Thought Leaders

Check Point®
SOFTWARE TECHNOLOGIES LTD

ISMG
INFORMATION SECURITY
MEDIA GROUP

Tom Field
Vice President, Editorial

About the 2017 Ransomware Defense Survey

Fifty-two percent of security leaders rate their organizations at above average or superior when it comes to detecting or blocking ransomware before it locks or encrypts data in their systems.

Yet, 36 percent also say their organizations were victims of ransomware in the past year. And 57 percent say they are more likely to be a ransomware target in 2017.

These are among the results of the 2017 Ransomware Defense Survey. Aimed at determining the true impact of ransomware on organizations across industries, the survey uncovers some stark contrasts, such as:

- 76 percent see ransomware as a significant business threat, vs. an over-hyped news story (5 percent).
- Yet only 56 percent say they currently have a ransomware response plan.

And although 74 percent of respondents believe professional criminals pose the greatest ransomware threat to their organizations, and 21 percent say ransomware is evolving in menacing new ways, 44 percent say that users remain the single weakest link in their security chain.

How will organizations fortify their defenses in 2017? What can they do to prevent and detect ransomware before it takes root and cripples their operations? Read on for full survey results, as well as expert analysis of how to put this information to use to improve your organization's ransomware defenses.

Best,

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com

About this survey: This survey was conducted online in the fall of 2016, and it generated more than 230 responses from organizations primarily in the U.S., Asia, Canada and the UK. Seventy percent of respondents are from organizations of 1,000 to 2,000 employees. Respondents represent many industry sectors, but primarily professional services, healthcare, high tech and financial services.

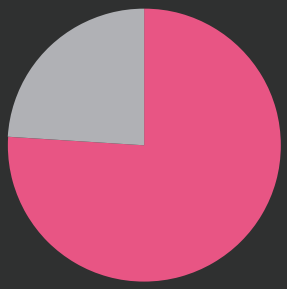
About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest network cybersecurity vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises—from networks to mobile devices—in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

Check Point®
SOFTWARE TECHNOLOGIES LTD

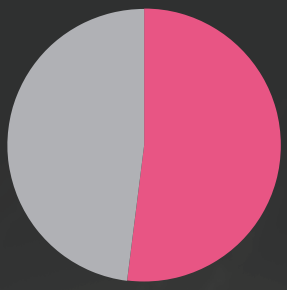
By the Numbers

Some statistics that jump out from this study:



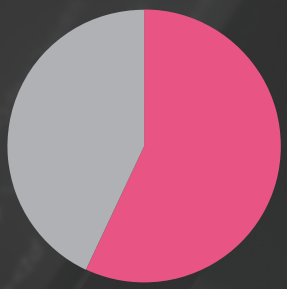
76%

of respondents see ransomware as a significant business threat.



52%

rate their organizations at above average or superior when it comes to detecting or blocking ransomware before it locks or encrypts data in their systems.



57%

say they are more likely to be a ransomware target in 2017.

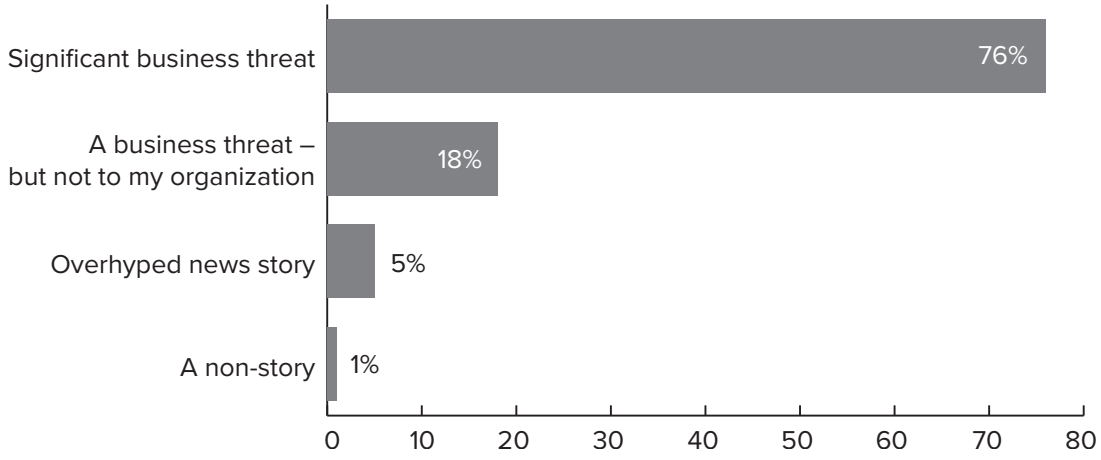
Ransomware Pulse

In this opening section, the survey results show how organizations currently view the ransomware threat – whether as a significant business challenge or an overhyped news story. Some key statistics:

- 76 percent of respondents see ransomware as a significant business threat to enterprises such as their own.
- 52 percent say their capabilities to block or detect ransomware are average or superior when compared to peers.

Read on for more perspectives.

1. In your opinion, is ransomware currently a significant business threat to enterprises such as your own, or is it more of an overhyped news story?

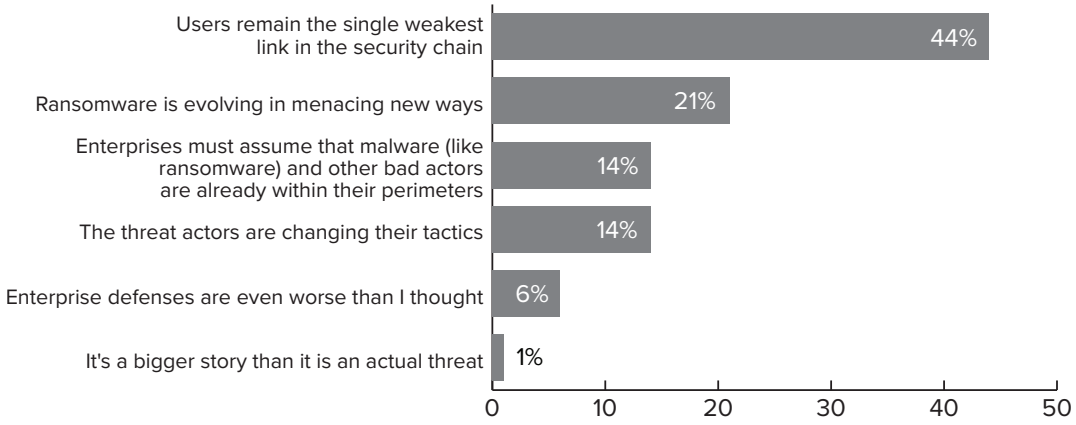


No question, ransomware dominated the headlines in 2016. People talked worldwide about the Hollywood Presbyterian Medical Center case and whether organizations should or should not pay the ransom when attacked. But was the ransomware story overhyped?

Not according to survey respondents. Asked whether ransomware represents a significant business threat, 76 percent said yes, versus 5 percent who said it is an overhyped news story.

Asked whether ransomware represents a significant business threat, 76 percent said yes, versus 5 percent who said it is an overhyped news story.

2. What do you believe to be the biggest takeaway from the ransomware surge in 2016?

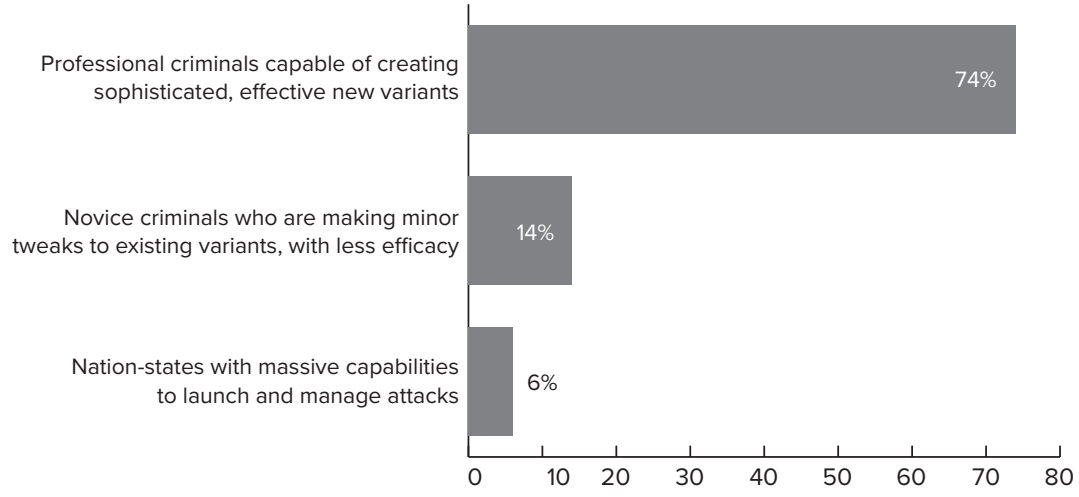


So, if ransomware is such a threat, then what do security leaders take away from this year's incidents? For 44 percent of respondents, the message is: users remain the single biggest weakness in the security chain, as they tend to be the ones introducing ransomware to the organizations.

Other key responses:

- 21 percent say ransomware is evolving in menacing new ways
- 14 percent say threat actors are changing their tactics

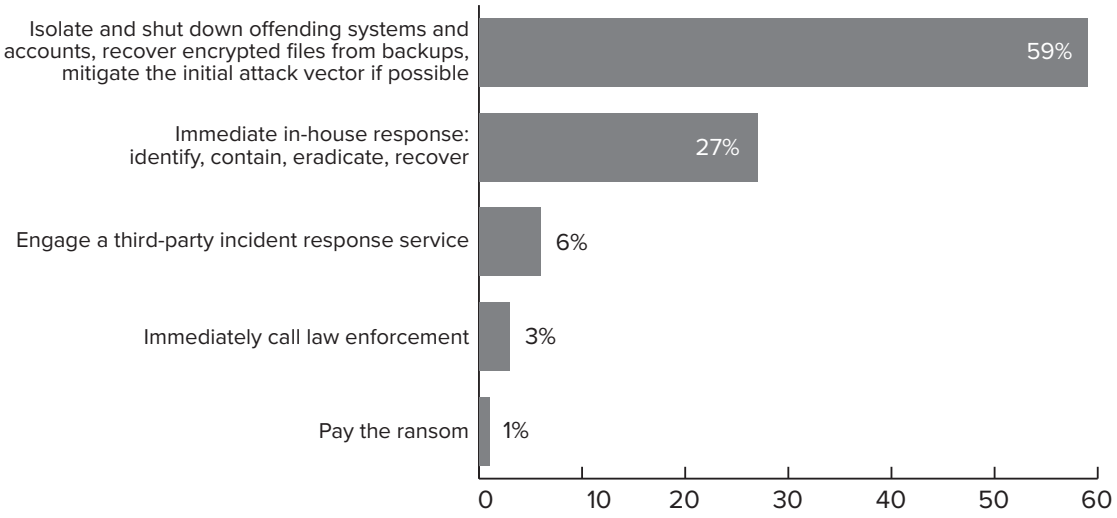
3. Based on what you know about ransomware, who do you believe are the predominant threat actors behind the attacks?



And respondents are clear about whom they believe to be the predominant threat actors behind the attacks. The culprits are professional criminals who are capable of creating sophisticated, effective new variants, according to 74 percent of respondents.

Fourteen percent attribute these attacks to novice criminals who are making minor tweaks to existing variants, while 6 percent point the finger at nation states.

4. How do you believe organizations should respond when they detect ransomware that has maliciously impacted their systems?

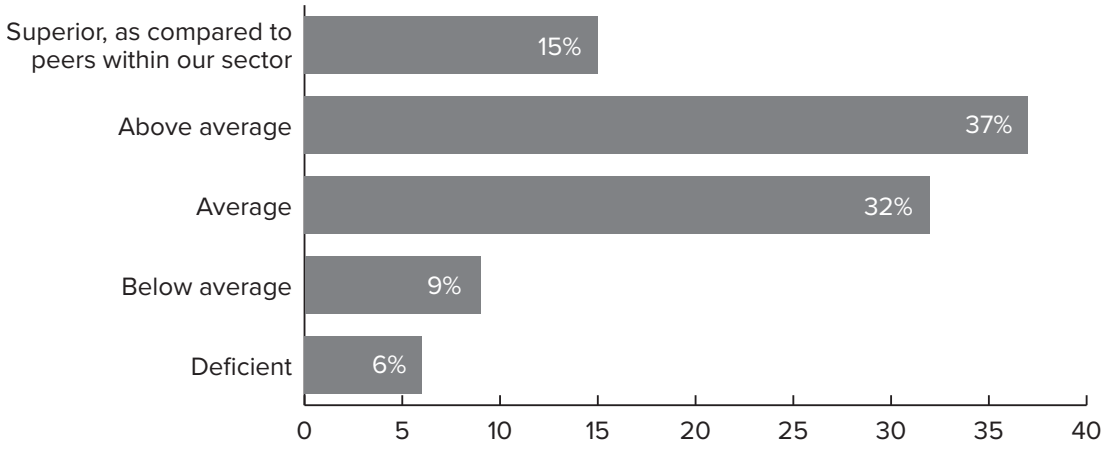


Should organizations simply pay the ransom when they detect ransomware that has maliciously impacted their systems? No, not at all, say 99 percent of respondents.

Top responses include:

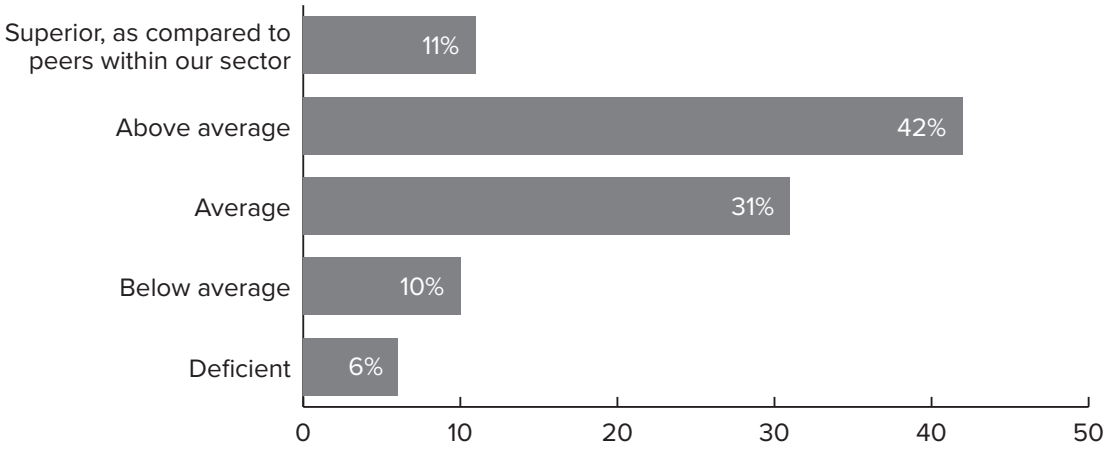
- Isolate and shut down offending systems and accounts, recover encrypted files from backups, mitigate the initial attack vector if possible – 59 percent
- Immediate in-house response: identify, contain, eradicate, recover – 27 percent

5. How do you assess your organization's current ability to either block or detect ransomware *before* it locks or encrypts data within your systems?



To baseline ransomware defenses, respondents were asked to self-assess their organization's current ability to either block or detect ransomware before it locks or encrypts data within their systems. Fifty-two percent rate themselves at above average or superior; 32 percent say they are average, as compared to peers.

6. How do you assess your organization's current ability to either quickly block or detect ransomware *after* it locks or encrypts data within your systems?



Next, they were asked: How do you assess your organization's current ability to either quickly block or detect ransomware after it locks or encrypts data within your systems?

This time, 53 percent grade themselves above average or superior, while 31 percent say they are average.

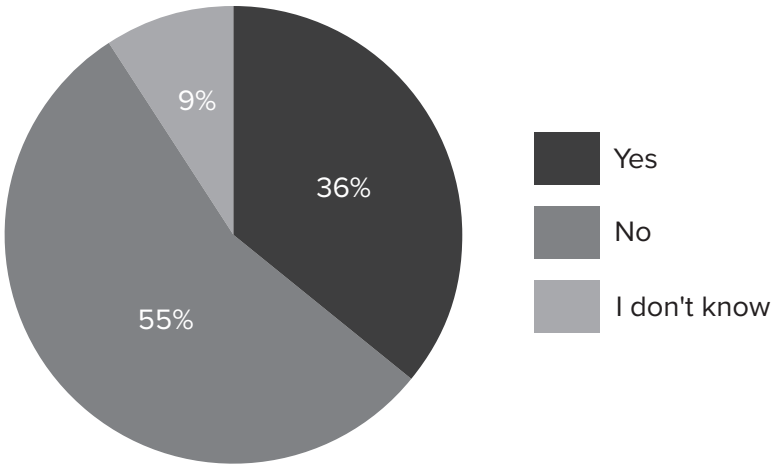
Up next: The business impact of ransomware.

Ransomware Impact

So, ransomware is seen as a significant threat, but has it manifested itself as one for our survey respondents?

- 36 percent say they know they have been a victim of ransomware in the past year
- 64 percent of those victims say their top business impact was “loss of productivity.”

7. Has your organization in the past year fallen victim to ransomware?

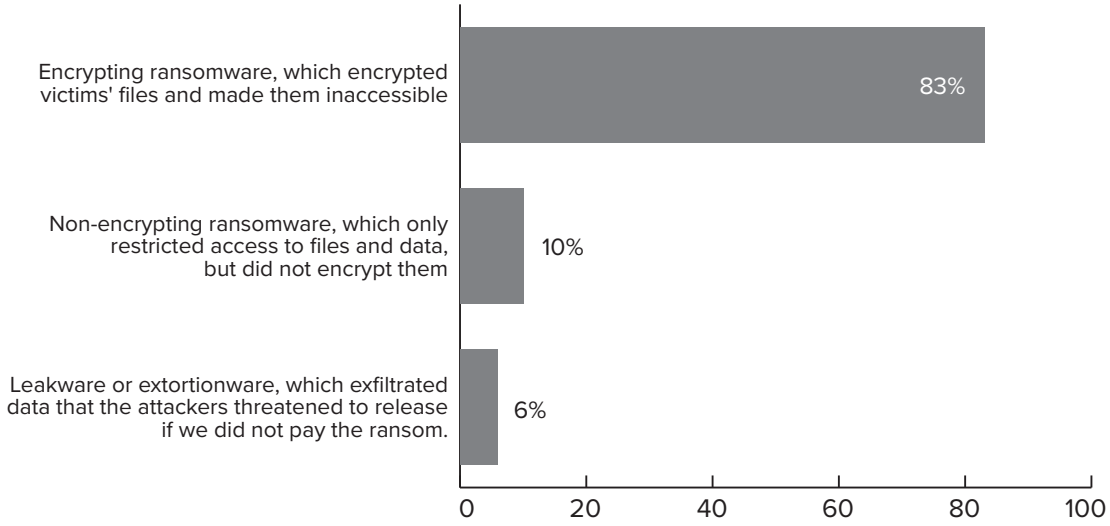


While more than half of respondents say their organizations were not ransomware victims in the past year, nearly 10 percent claim they do not know, which raises the prospect that the percentage of those who say they were victims—36 percent—could, in fact, be higher.

Of those who know they were ransomware victims, what else can they report?

While more than half of respondents say their organizations were not ransomware victims in the past year, nearly 10 percent claim they do not know.

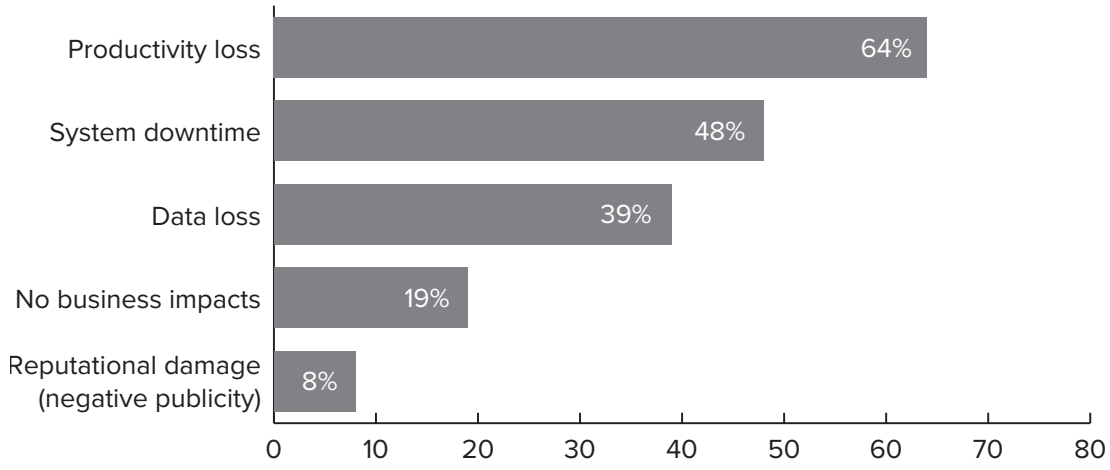
8. If you answered yes to the previous question, what type of ransomware infected your organization? (select all that apply)



Eighty-three percent say they were struck by encrypting ransomware, which encrypted victims' files and made them inaccessible.

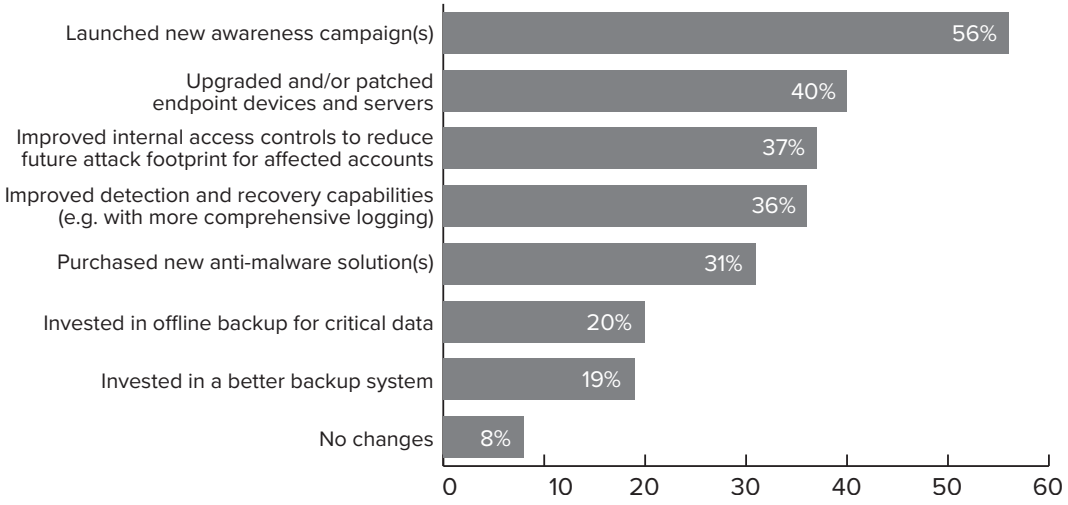
Only 10 percent report being struck by non-encrypting ransomware, which restricts access to files and data.

9. If you answered yes to question #7, what business impacts did your organization experience as a result of ransomware infection? (select all that apply)



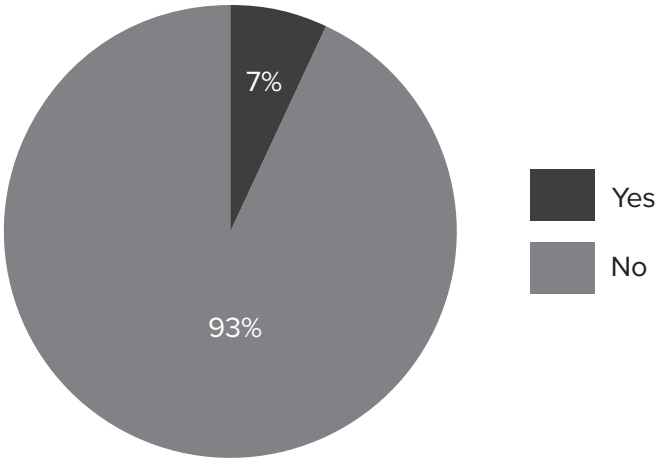
In terms of business impact, 64 percent report a productivity loss, while 48 percent say they saw system downtime, and 39 percent cite data loss.

10. If you answered yes to question #7, what changes, if any, did your organization initiate as a result of the ransomware threat? (select all that apply)



As a result of ransomware attacks, 56 percent of respondents say they launched new awareness campaigns, while 40 percent say they upgraded and/or patched endpoint devices and servers. Thirty-seven percent say they improved internal access controls to reduce the future attack footprint for affected accounts.

11. Again, if you answered yes to question #7, did you ever pay the ransom?



But did they pay the ransom? Mostly not. Only seven percent say they paid a ransom, while the remaining 93 percent say “no.”

12. Open-ended: In your experience, what would you estimate as the total cost of a ransomware infection—from detection to mitigation to business impact?

It's difficult to estimate the total cost of a ransomware infection. Respondents were asked an open-ended question on the topic, and the responses: 2 bitcoins to $500 to $1 million or more. One respondent says: “depends how early it is detected, but could be $300k to $3M.”

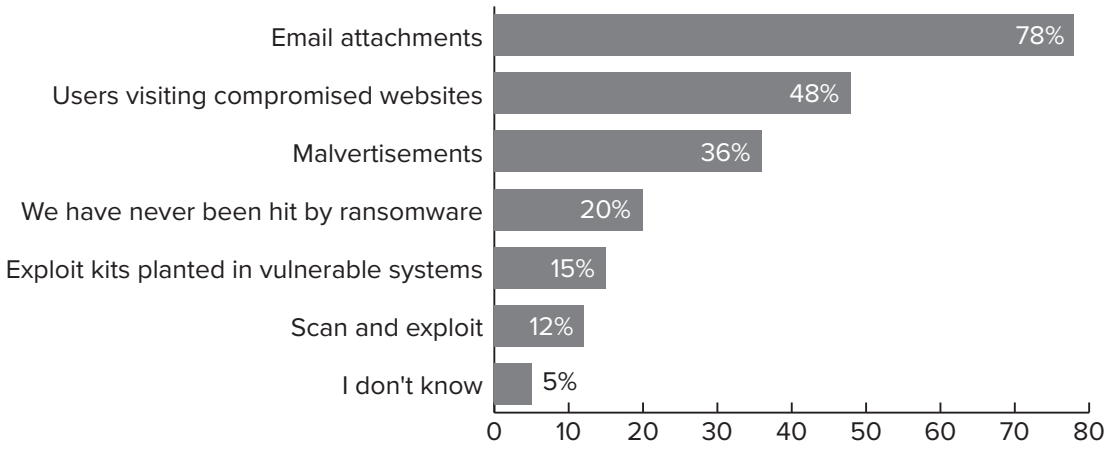
Up next: Ransomware detection.

Detection

This section examines how ransomware typically enters organizations, as well as how effectively it is detected. Some highlights:

- 78 percent say ransomware typically enters organizations via email attachments
- Only 21 percent say they are extremely confident that their organization's defenses are capable of detecting malware on endpoint devices before it spreads

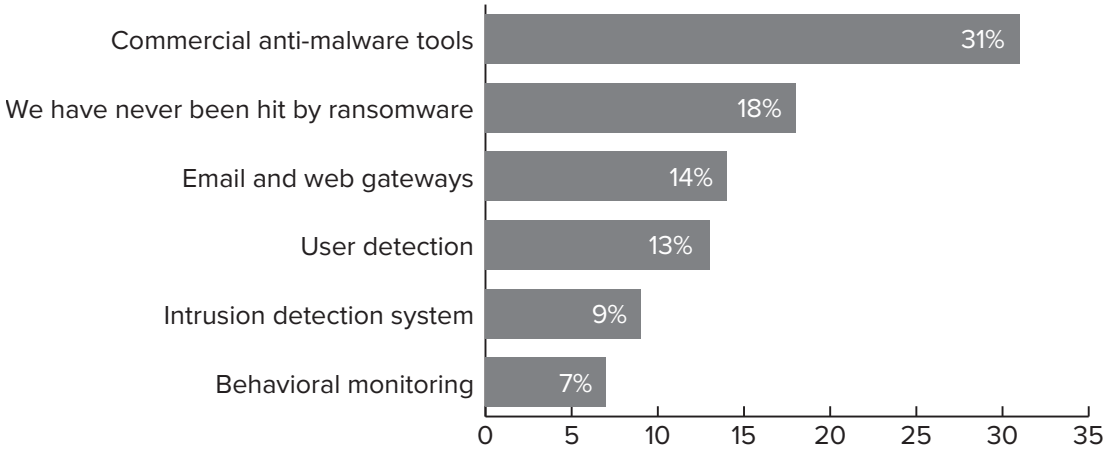
13. How does ransomware typically try to enter your organization? (select all that apply)



Email attachments are the most common way that ransomware typically enters organizations. But it's hardly alone. Respondents also say that ransomware commonly enters via users visiting compromised websites (48 percent) and through malvertisements (36 percent).

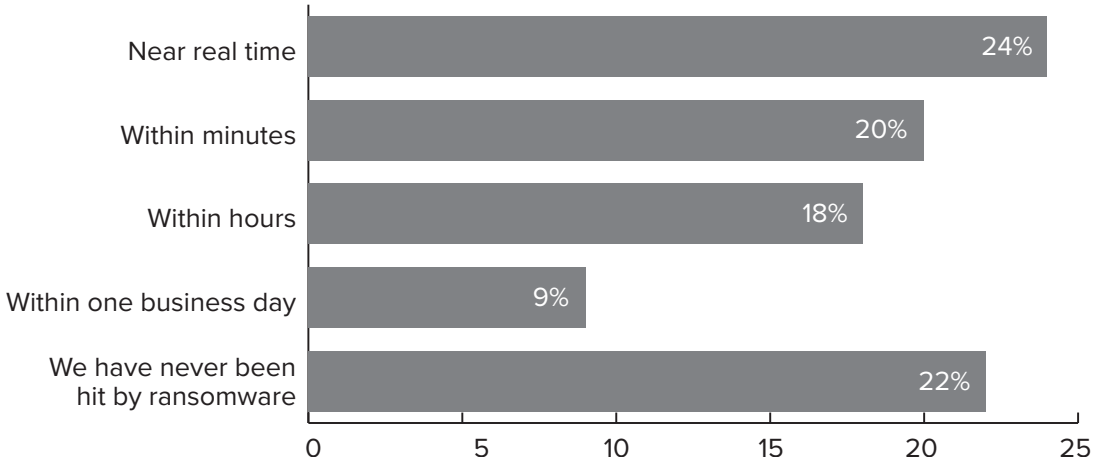
Email attachments are the most common way that ransomware typically enters organizations.

14. How is ransomware typically detected when it attempts to enter your organization?



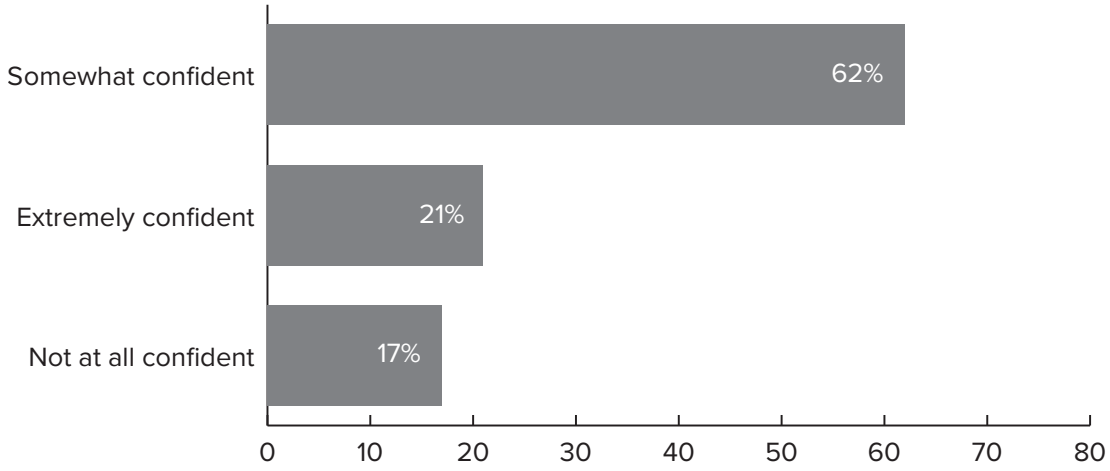
How is ransomware typically detected? The most common way is by using commercial anti-malware tools, according to 31 percent of respondents. Fourteen percent detect it via email and web gateways, while 13 percent say it is through user detection.

15. How quickly is ransomware typically detected when it attempts to enter your organization?



As for how quickly ransomware is detected, nearly one-quarter of respondents say it is near real-time, while one-fifth say within minutes.

16. How confident are you that your organization's defenses are capable of detecting malware on endpoint devices before it spreads from workstations and infects critical files via file-share?



Asked about their level of confidence in the capability of their organization's defenses to detect malware on endpoint devices before it spreads from workstations and infects critical files via file-share, only 21 percent are extremely confident. Sixty-two percent say they are somewhat confident, while 17 percent say they are not at all confident.

The next section focuses on malware remediation.

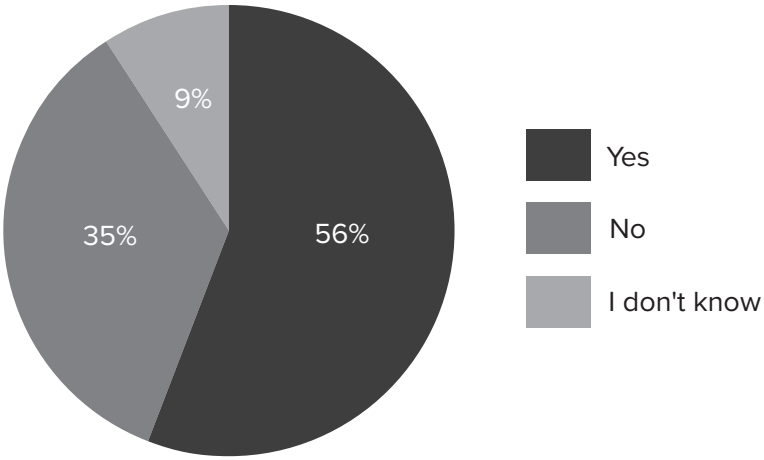
Asked about their level of confidence in the capability of their organization's defenses to detect malware on endpoint devices before it spreads from workstations and infects critical files via file-share, only 21 percent are extremely confident.

Remediation

When it comes to ransomware remediation, there is plenty to be concerned about. Here are two sobering stats:

- Only 56 percent of organizations currently have a ransomware response plan in place.
- Only 21 percent say their current anti-malware solution is completely effective at protecting their organization from ransomware.

17. Does your organization have a ransomware response plan in place?

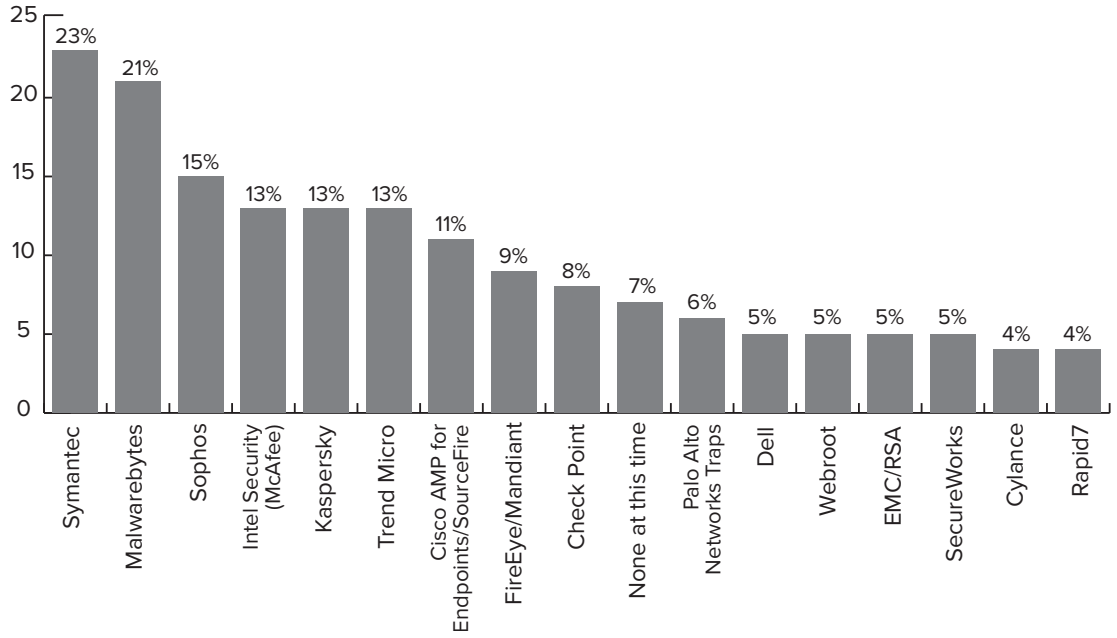


Given that three-quarters of respondents see ransomware as a significant issue, you might expect a similar response to the question: Does your organization have a ransomware response plan in place?

But, in fact, barely half of respondents say they have such a plan. Thirty-five percent say they do not have a plan, while 9 percent do not know.

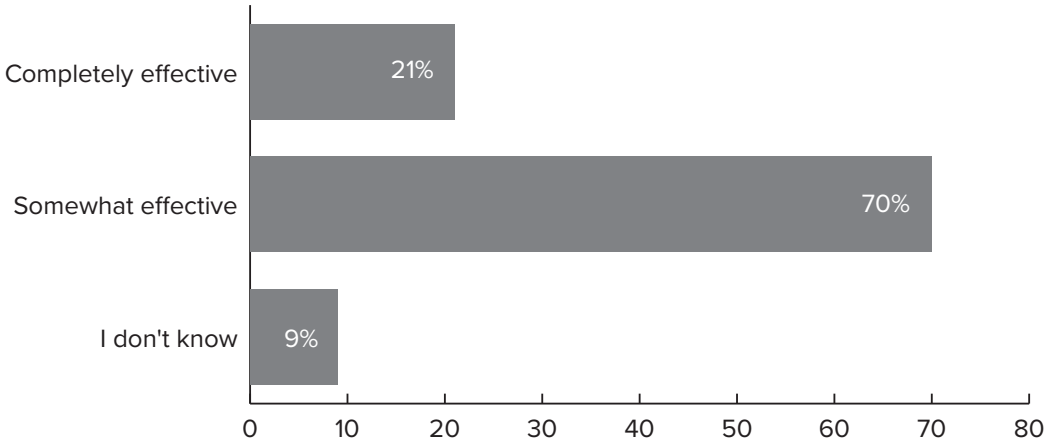
Thirty-five percent say they do not have a ransomware response plan, while 9 percent do not know.

18. Which of these vendors do you currently use for ransomware protection? (select all that apply)



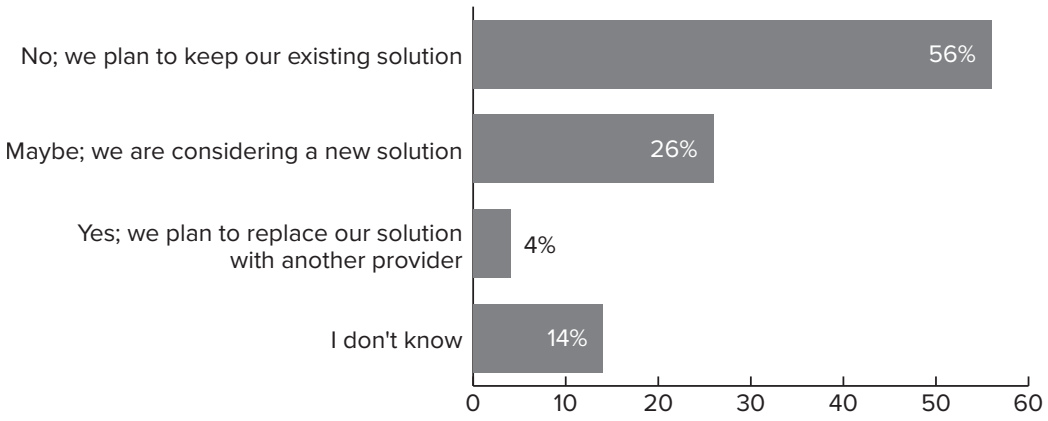
Respondents were asked to name which vendors they currently use for ransomware protection. The list is long, and emerging at the top are: Symantec (23 percent), Malwarebytes (21 percent) and Sophos (15 percent).

19. How effective do your believe your current anti-malware solution is at protecting your organization from ransomware?



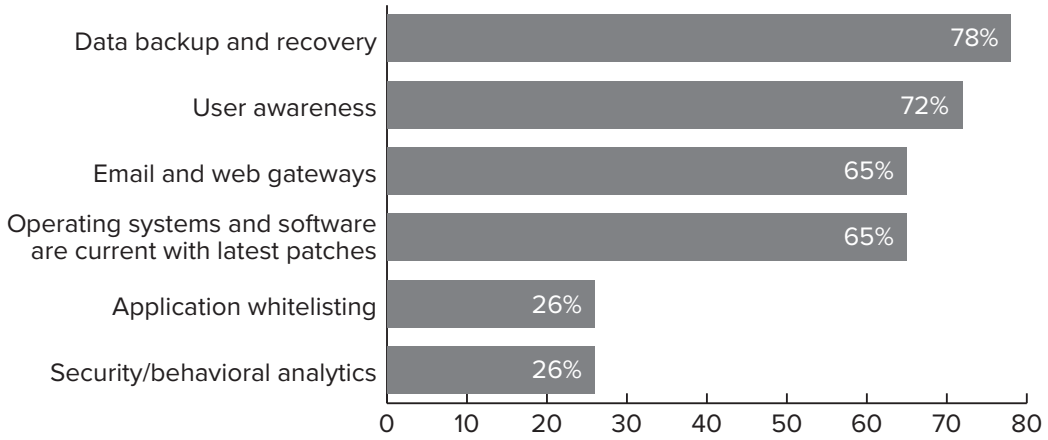
But despite the wide usage of anti-malware vendors, only 21 percent of respondents say their current solutions are completely effective at protecting organizations from ransomware. Seventy percent say the current solutions are only somewhat effective.

20. Has a ransomware outbreak caused your organization to consider replacing its existing AV/endpoint security solution?



Dissatisfaction is no call to arms, though. Only 4 percent of respondents say ransomware has caused their organization to consider replacing its existing AV/endpoint security solution. Fifty-six percent, in fact, say "no; we plan to keep our existing solution."

21. What other security solutions do you currently employ to combat ransomware? (select all that apply)



Beyond anti-malware and endpoint security solutions, what other controls are organizations currently employing to fight ransomware? The most common responses:

- Data backup and recovery – 78 percent
- Updated patching – 72 percent
- Email and web gateways/behavioral analytics – both at 65 percent

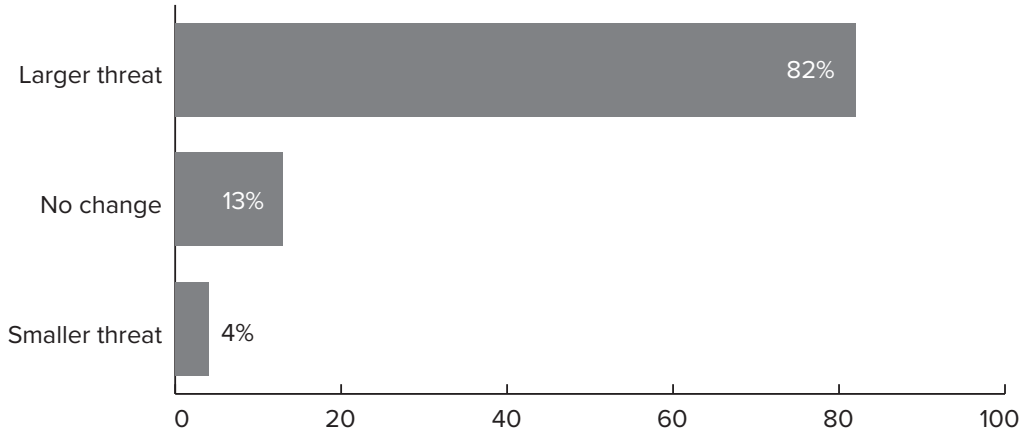
Upcoming: A look at 2017 anti-ransomware budgets and plans.

2017 Anti-Ransomware Agenda

Given the significance—and recognition—of ransomware as a growing threat to organizations across sectors, how are defensive plans shaping up? Well …

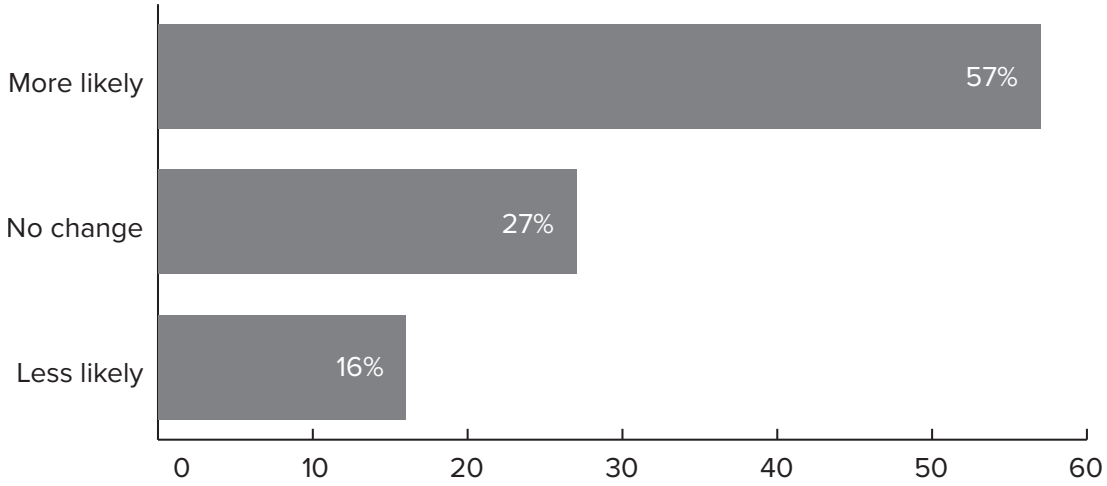
- 82 percent of respondents believe ransomware in 2017 will be a larger threat to organizations globally
- 97 percent will have either the same or an increased budget to fight ransomware

22. In 2017, do you believe ransomware will be a larger or smaller business threat to organizations globally?



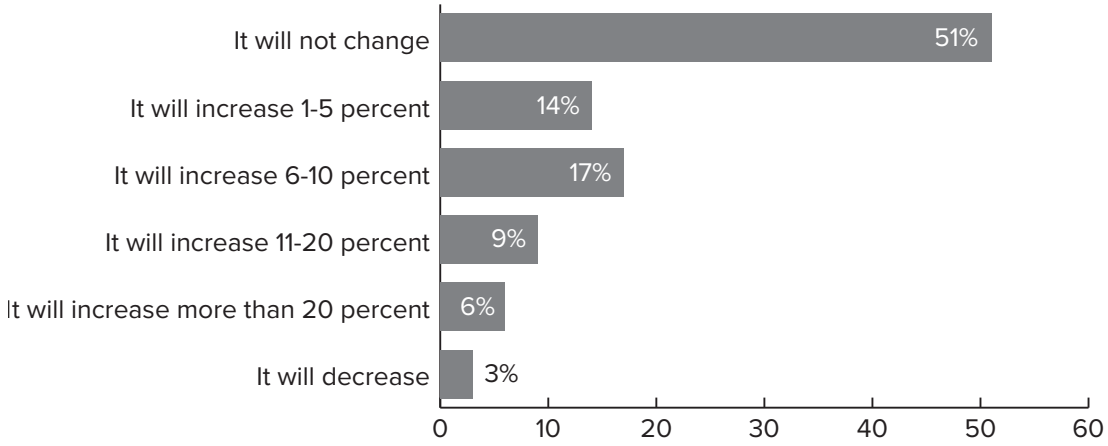
Asked whether they believe ransomware will be a larger or smaller business threat globally in 2017, only 4 percent say "smaller." The remainder see it as either a larger threat or no change from 2016.

23. Do you believe *your* organization will be more or less likely to be a target of ransomware?



Asked whether their own organizations are more or less likely to be a ransomware target in 2017, 84 percent said more likely or no change from 2016.

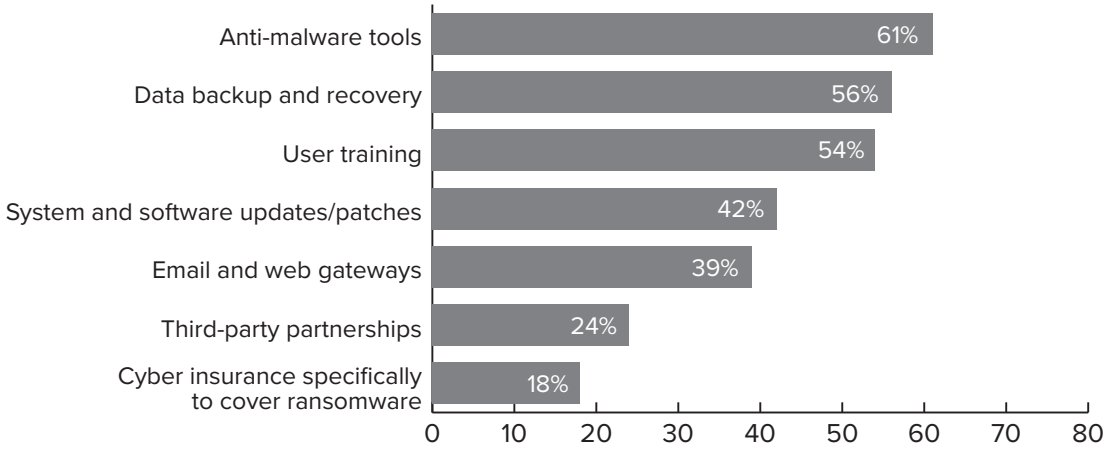
24. How do you expect your organization's budget for ransomware security to change?



Some 46 percent of organizations expect their budget for ransomware security to grow in 2017. Of those, most expect an increase of 6 percent or more.

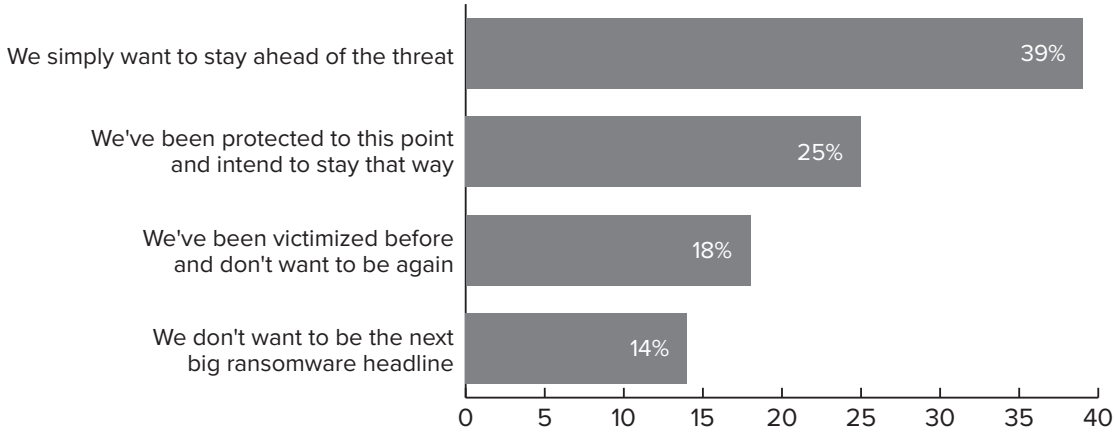
How will those funds be allocated?

25. What specific ransomware-related cybersecurity investments do you expect your organization to make in 2017? (select all that apply)



Sixty-one percent expect to invest more in anti-malware tools, while 56 percent are eyeing data backup and recovery, and 54 percent expect to spend more on user training. Bottom line: They expect to do more of what they are already doing to fight ransomware.

26. What will be your organization's primary driver for improving ransomware defense?



Asked what is their organization's primary driver for improving ransomware defense, 39 percent said they simply want to stay ahead of the threat, while 25 percent say "We've been protected to this point and intend to stay that way."

Eighteen percent say they have been victims before and don't want to be again.

27. Open-ended: What one factor do you believe could have the greatest impact on defeating ransomware in 2017?

Finally, the survey concludes with an open-ended question: What one factor do you believe could have the greatest impact on defeating ransomware in 2017?

Responses range from awareness/education to "don't pay the ransom" and "backups, backups, backups," as well as prosecution of ransomware actors. The most common response is about somehow improving user awareness.

In the next section, the report spells out conclusions about the survey results.

Conclusions

In reaching conclusions about the survey results, it is important to review the statistics shared at the very beginning of this report:

- 76% of respondents see ransomware as a significant business threat.
- 52% rate their organizations at above average or superior when it comes to detecting or blocking ransomware before it locks or encrypts data in their systems.
- 57% say they are more likely to be a ransomware target in 2017.

The disconnect is even more alarming when one has all of the survey results for context. Three-quarters of survey respondents say ransomware is a significant business threat, and more than half believe they are more likely to be a target for attack in 2017. Yet, only 56 percent have a ransomware response plan in place, and 48 percent believe their organizations are average at best when it comes to detecting or blocking ransomware before it locks or encrypts data in their systems.

At a time when industry researchers are discovering scores of new ransomware variants, and when the capabilities to launch such attacks are more accessible to threat actors than ever before … organizations across sectors need to take ransomware far more seriously.

Some survey conclusions to consider:

1. *Act* Like Ransomware is a Serious Business Threat

It is remarkable 1) that 24 percent of respondent organizations don't see ransomware as a serious business threat, and 2) that barely half of them have a ransomware response plan in place. Given the spread of these attacks—as well as their success across industry sectors and global regions—there is no excuse for not being prepared. Need help framing the business case? Don't cite Hollywood Presbyterian Medical Center, which paid the ransom to regain access to its data. Instead, think back to Sony Pictures, where attackers exploited similar vulnerabilities and were able to erase critical data. Can your organization withstand such a blistering attack? That is the argument for a response plan.

2. It's Time to Upgrade the Defenses

Acknowledging the problem is a solid step forward, and 79 percent of survey respondents acknowledge that their current anti-malware solution is not completely effective at protecting their organization from ransomware. But what are they going to do about it? That is the key question. And the answer is distressing: Only 4 percent of respondents say ransomware has caused their organization to consider replacing its existing AV/endpoint security solution. Then, when you look at investment plans for 2017, the top responses are "more of the same"—anti-malware, backup and the ubiquitous "user awareness." The evolution of ransomware represents a new challenge to many organizations, and it demands a new defensive strategy. Attackers are continually changing their game in response to security controls. That means security leaders need to change their games, too. Beyond fundamental anti-malware controls, organizations must do a better job authenticating incoming email, spotting suspicious attachments at the gateway, monitoring internal traffic for anomalous activity and responding to alerts in real time to detect and defeat ransomware before it does damage.

3. There are no "Buts" in "Don't Pay the Ransom"

To paraphrase a well-worn bit of philosophy, all that is necessary for ransomware attackers to succeed is for well-meaning organizations to pay the ransom. In 2016, it became common for thought leaders to say "Never pay the ransom, but …," and that "but" was meant to allow wiggle room for instances when a $500 ransom was cheaper than the hassle of not paying, or when healthcare entities were dealing with true matters of life and death. But the problem with either of those scenarios is: As soon as one pays the ransom, then one has reinforced that the attackers made the right decision to attack. The only reason this crime thrives is because it's profitable—organizations (despite what they say publicly) continue to pay the ransom. When that stops, so will the attacks.

‘Ransomware is Taking Over …’

Survey Analysis by Orli Gan of Check Point Software Technologies

NOTE: *In preparation of this report, ISMG Vice President of Editorial Tom Field sat down with Orli Gan of survey sponsor Check Point Software Technologies to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.*

Survey Results Overview

TOM FIELD: Orli, you’ve had the chance to review the survey results. How would you say that overall the results either validate or challenge the hypotheses you may have had going into the research project?

ORLI GAN: The results are validating—ransomware is affecting everyone. It’s a very real problem, and it’s gone way beyond the media hype. It is very much a real problem that organizations, regardless of size and industry, are dealing with on a daily basis.

The one response that kind of stood out for us is the high value that people give to user’s education. And while we certainly do think it’s good practice to teach your people not to click on just any random attachment, we also truly believe that if you focused on that, it means that you’re basically not trusting technology to help you. Ultimately every person—even the most established security professionals in the world—will at some point in time fall victim to something that they inadvertently clicked on. The social engineering aspect is becoming ever more sophisticated to the point where even a very trained person will find it hard to determine that this is something that is best left alone.

Overconfident?

FIELD: One of the things that struck me, reviewing the results, was the high level of confidence that respondents have in their own ransomware defenses. In your opinion, do they have maybe some overconfidence in these defenses? And if so, what would you say fuels that?

GAN: Yes, certainly we believe that most organizations—and we have the statistics to show that—are actually not as sophisticated as they may consider themselves to be, simply because they use dated technologies that are not as effective as they would like to think that they are to protect themselves against these modern, sophisticated threats. Ransomware has specific characteristics, which can only be combatted with dedicated anti-ransomware protection technology. Also, I think that what you see is overconfidence in whether they’re likely to be a victim. In fact we know that there is no industry, no company size that would make you immune. Everybody is a potential victim.


Orli Gan

“Ransomware is very much a real problem that organizations, regardless of size and industry, are dealing with very much on a daily basis.”

"We know that there is no industry, no vertical, no company size that would make you immune. Everybody is a potential victim."

Current Defenses

FIELD: How realistic are they about their likelihood of being targeted, and how adequate would you say are their current defenses?

GAN: Every year that goes by, they are more likely to be targeted. If you look at the cybercrime "industry," you can see its evolution. You can see that maybe two, three years ago, they were trying just to get their hands on the large amounts of data, or large numbers of credentials that would get them to enter places. And that still happens to a large degree today with all of the recent attacks we've all heard of at Yahoo! and with Check Point's recent discovery of the compromise of a million Google accounts.

But the cybercrime industry has gone a very long way from that point to understanding that the quickest way to monetize cybercrime is through ransomware. And this is where we see a very rapid and peaked increase in the amount of ransomware attacks as a whole and also as a percentage of the cybercrime in general. And we expect this to grow even more dramatically in 2017 and moving forward, simply because this has been a lucrative line of cybercrime business. It's very immediate, it's very impactful. You have a very good return on the investment, if you will.

People consider most of their ransomware attackers to be professional, sophisticated criminals. It's gone way beyond that. There are affiliation programs that would let even a very novice, smalltime criminal or even just a young person with a lack of judgment to create their own line of ransomware income.

As long as you care about your data, you are a target because you will pay good money to get it back. How adequate are their current defenses? I would say that they're a little over-optimistic, most of them, because we know the statistics on how many companies have actually adopted the more advanced, sophisticated defenses that would in fact be able to combat modern-day ransomware. And those statistics are not in line with the statistics that we show of customers thinking that they have relatively good defense.

Types of Ransomware

FIELD: How would you say the statistics about types of ransomware and infection points match what you typically see in the field?

GAN: I think those are fairly similar to what we see, that the vast majority of ransomware is in fact targeting files and encrypting files. You do see new variants surfacing over time—the types that have locked the user out. You have also mentioned leakware and extortionware, and those would be rare, first of all, because they only apply to a much smaller percentage of the businesses that would even mind that. "If you took my pictures, I don't care. If you want to post them, I'm not going to pay you anything; go ahead and post them." And that's true for a lot of other types of data where not having access to that data is still the most clear and present danger that people are afraid of. This is also where ransomware guys are making sure you're locked out of your data; therefore, you're very likely to pay them if you don't have a very good backup system in place.

Bolstering Anti-Malware Controls

FIELD: The respondents expressed that they lack confidence in their current anti-malware solutions to protect their organizations from ransomware. How do you recommend that they bolster these defenses?

GAN: For some decades now, we've been pitching the layered approach for security. And I actually think that this still remains very much the most respected defensive strategy for anyone, because you should not expect to have a single point solution placed on some strategic place that would solve all of your problems. The only true security solution is through a layered approach that takes into consideration the different vectors, the different elements, and ensures that you're covered from every different perspective. And that starts with a rigorous plan of patching your systems continuously, not just after you've been attacked. Because unpatched systems are the very first place that an attacker would look for.

You might also want to consider adopting mechanisms such as the Check Point Threat Extraction, which is a very proactive way to eliminate threats, simply by eliminating

the vehicles of delivery from the documents. You get a very safe version of the documents, which doesn't interfere with your business routines and yet really leaves the risk at the door.

We now also have a new generation of dedicated ransomware protection technologies for endpoints, built specifically to prevent these attacks. Our own Anti-Ransomware technology, a part of Check Point SandBlast Agent product, is an excellent example: It detects and quarantines unknown ransomware that can bypass other protections. If any data is encrypted as part of the attack then it's restored automatically.

The Weak Link

FIELD: How should security leaders address this issue of the users? Because, clearly, past efforts have not been affected.

GAN: It's probably good practice to educate users, but do not consider them to be your [only] line of defense. Because the criminals understand users very well, and therefore are becoming ever more sophisticated in making sure that they are able to entice them into double-clicking with ways that we see becoming ever more sophisticated and ever more personalized, to the point that even a very savvy, educated person would find it very hard to understand that this is something rogue.

A recent attacker for ransomware will offer you an opportunity to either pay the ransom or to infect two of your friends. Now, other than that being a very cruel type of pyramid operation, what that means is that if your friend chose the path of infecting his friends, you're now getting an email from somebody that you truly know that's coming from your real emails.

So this is just to give you an idea of the level of sophistication that we have come to expect, and we continue to be amazed to see more of it coming from the criminal side. And if you think about that, if you think that the business is going to grow, you need to be aware that you absolutely have to have the security, technological measurements in place. You should not be angry at the person who double-clicks, for the most part, because they are supposed to be assured that their business assets are safe to use and not have to constantly be reminded maybe this thing is carrying something that it shouldn't.

Ransomware Trends to Watch

FIELD: As we start 2017, what are some of the ransomware trends that you observe and maybe concern you the most?

GAN: First and foremost, ransomware is taking over simply because this is the most lucrative line of cybercrime out there. As people, we think that law

enforcement agencies are pretty much helpless. So even though this is very much a crime, it's not treated as a crime by the rest of the world. It's still considered very much a nuisance to the people who are affected by it, and this is very much concerning to us as we see the operations growing and becoming more sophisticated and being treated almost as a legitimate business.

So with that in mind, I think that we will see fewer professional type of criminals actually operating this, but they will start operating the infrastructure. There will be more smalltime criminals that are getting into those affiliation programs and starting their line of ransomware business. I am positive that we'll see more creativity into how you get users to become infected, whether it's through infect-your-friend type of things and other trends that we would see surfacing.

We expect to see the ransomware itself from a technological standpoint becoming more evasive, and therefore more immune to existing security systems. Which basically implies that if you're an organization, you cannot just assume last year's solution ... will still protect you next year.

I also think that we are likely to see more ways where you're being locked out. We pointed out the extortionware and leakware and other types of ways to lock you out of your data or to create something that would leave you to pay the ransom. I would expect to see again more creativity on the criminal side where they would find more ways that would cause you enough pain, especially if you're willing to pay, and those may not be things that you can overcome with just a simple recovery from backup.

Budgeting for 2017

FIELD: Orli, it was clear from our survey that the majority of respondents expect to see increases in their budgets for cyber security and ransomware in 2017. How do you recommend they approach allocating these funds?

GAN: I expect them to understand that there is no single magic bullet here that they can put into their organization and have this problem go away. There never was and there never will be, simply because the other side is continuously evolving. And with that in mind, I would expect them to go with a leader, with somebody who understands their needs and somebody that they know will be around not just today, but tomorrow and for the foreseeable future. When you consider the risk, when you understand how much you stand to lose, it makes it very easy to understand how you need to spend that budget, what would make it more effective, how much that you truly have, and how to distribute it across the various attack vectors and the methodologies used by the attackers. ■

Ransomware Resources

NOTE: From our vast content library, ISMG provides the following ransomware-related resources. Please visit any of our media sites for more news, views, education and industry insight.

San Francisco's Muni Vows: We Won't Pay Bitcoin Ransom

MATHEW J. SCHWARTZ

Score one for preparation: In the wake of a ransomware attack that infected 900 workstations, the San Francisco Municipal Transportation Agency says it's restoring affected systems, vowing to not give the attackers a single bitcoin of their ransom demand.

Read Article

Ransomware Attack on State Govt. Dept. Raises Concerns

VARUN HARAN

News that a state agency in India was the victim of a ransomware attack highlights the need for public and private sector organizations to promptly take appropriate action to mitigate their risks as hackers start going after low-hanging fruit.

Read Article

Is Ransomware Creeping Into Facebook and LinkedIn?

JEREMY KIRK

Facebook says it hasn't seen ransomware spreading through its Messenger instant messaging platform despite recent reports from researchers saying that the file-encrypting Locky may have slipped through.

Read Article

Ransomware Family Count Surpasses 200

MATHEW J. SCHWARTZ

Cybercriminals are continuing to refine their art: Researchers say there are now more than 200 ransomware families, which complicates ongoing attempts to disrupt such attacks.

Read Article

FBI: Why So Many Organizations Are Vulnerable to Ransomware

TOM FIELD

Ransomware has been one of the highest-profile cybercrimes of 2016, and the FBI has been at the heart of many investigations. Jay Kramer, a supervisory special agent with the bureau, discusses what he's learned about defending against ransomware in this video interview.

Watch Interview

After Ransomware Attack, Clinic Faces More Woes

MARIANNE KOLBASUK MCGEE

A recent breach reported by an Arlington, Texas-based pediatric clinic serves as the latest reminder of the substantial risks ransomware poses to patient data. The clinic offers advice to others based on difficulties it experienced in the response to the attack, and security experts also provide insights.

Read Article

FBI to Ransomware Victims: Please Come Forward

MATHEW J. SCHWARTZ

Have you been the target or victim of ransomware-wielding attackers? The FBI wants individuals and businesses to report ransomware attacks to help it better pursue, disrupt and potentially arrest suspects.

Read Article

Can't Stop the Ransomware

MATHEW J. SCHWARTZ

In their quest for easy ways to extort victims into giving them bitcoins, cybercriminals continue to double down on crypto-ransomware attacks and increasingly target enterprises, seeking proportionally higher paydays.

Read Article

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com

BANK INFO SECURITY® CU INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY®

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com