2017

RANSOMWARE DEFENSE SURVEY

The Enterprise Strikes Back

INSIDE:

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

VARONIS

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.

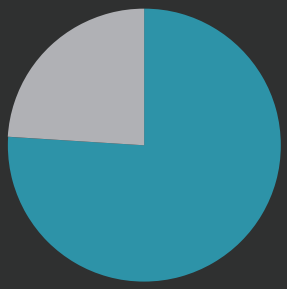
About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data, which often contain an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records.

For more information, visit www.varonis.com.

By the Numbers

Some statistics that jump out from this study:

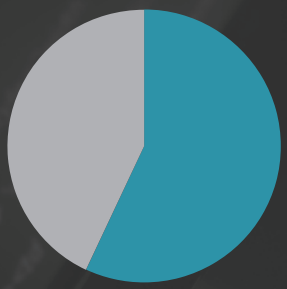


76%

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.

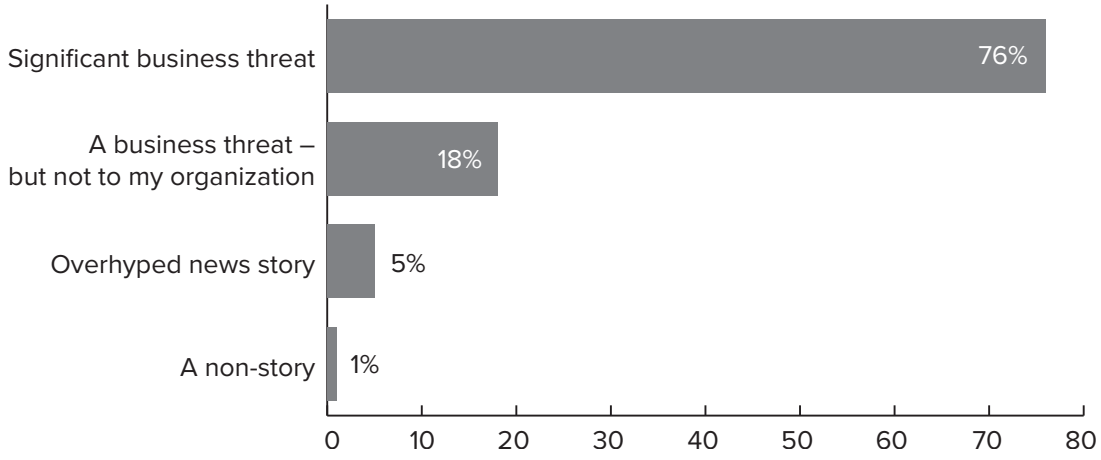
Ransomware Pulse

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?

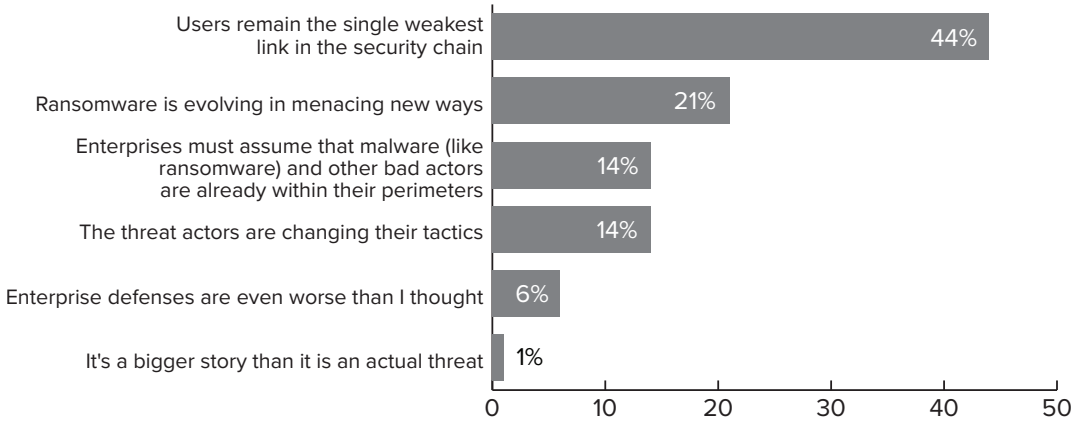


No question, ransomware dominated the headlines in 2016. People talked worldwide about the Hollywood Presbyterian Medical Center case and whether organizations should or should not pay the ransom when attacked. But was the ransomware story overhyped?

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?

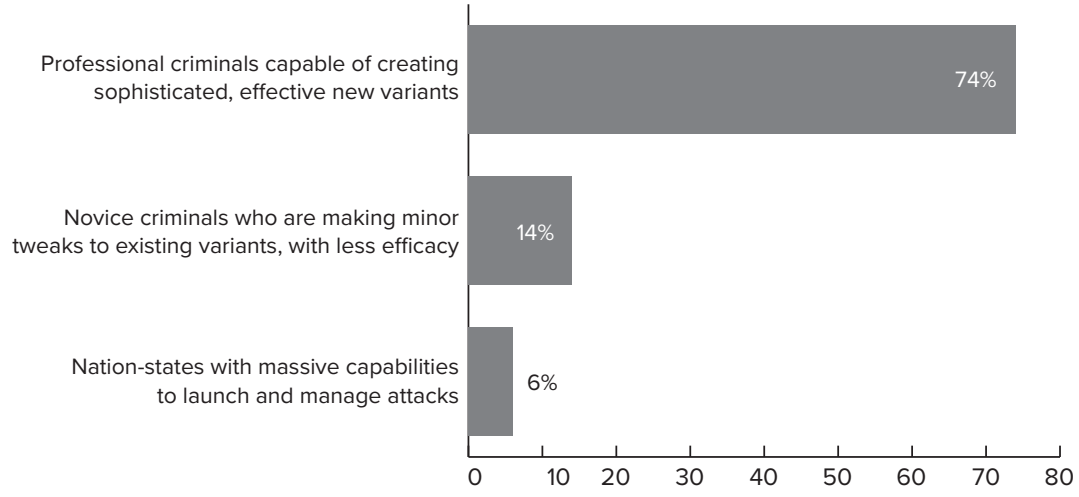


So, if ransomware is such a threat, then what do security leaders take away from this year's incidents? For 44 percent of respondents, the message is: Users remain the single biggest weakness in the security chain, as they tend to be the ones introducing ransomware to the organizations.

Other key responses:

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

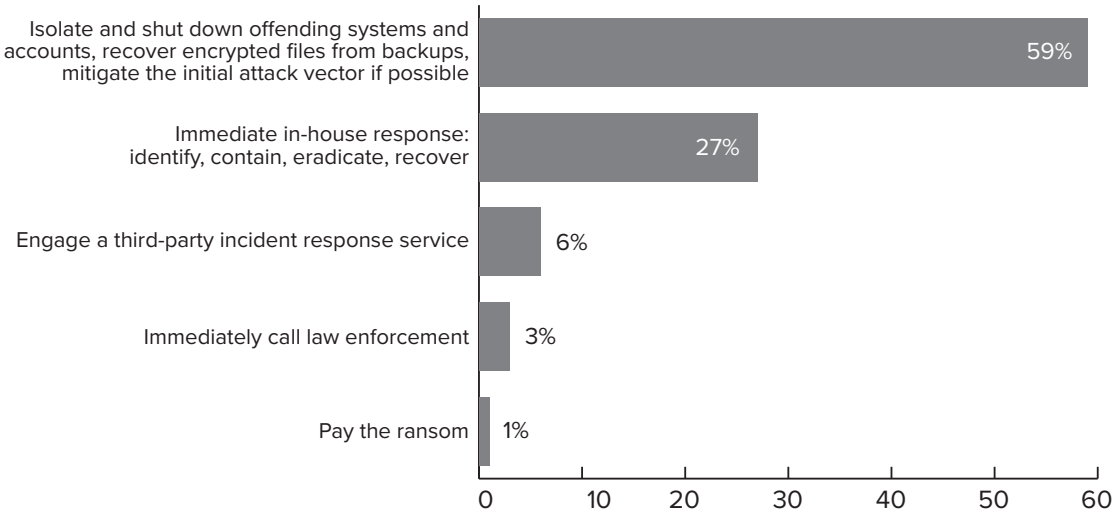
3. Based on what you know about ransomware, who do you believe are the predominant threat actors behind the attacks?



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?

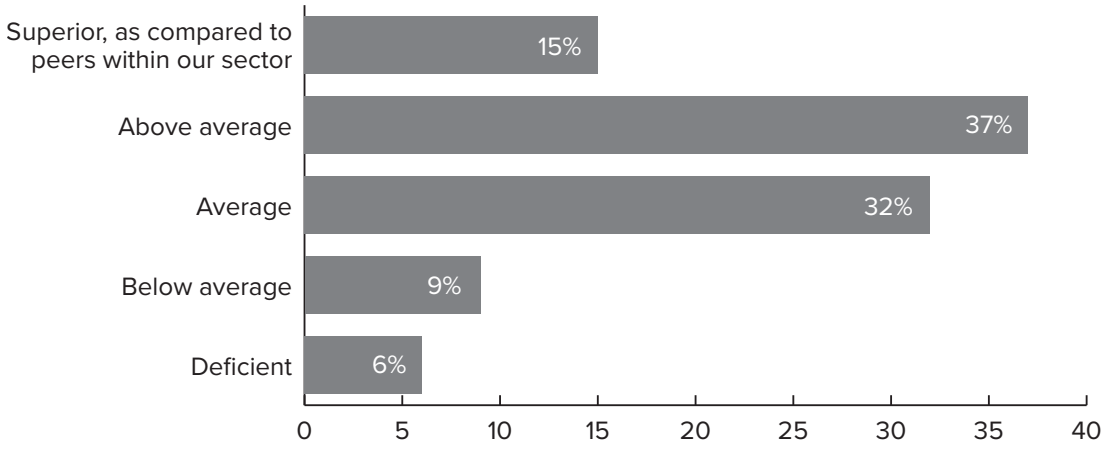


Should organizations simply pay the ransom when they detect ransomware that has maliciously impacted their systems? No, not at all, say 99 percent of respondents.

Top responses include:

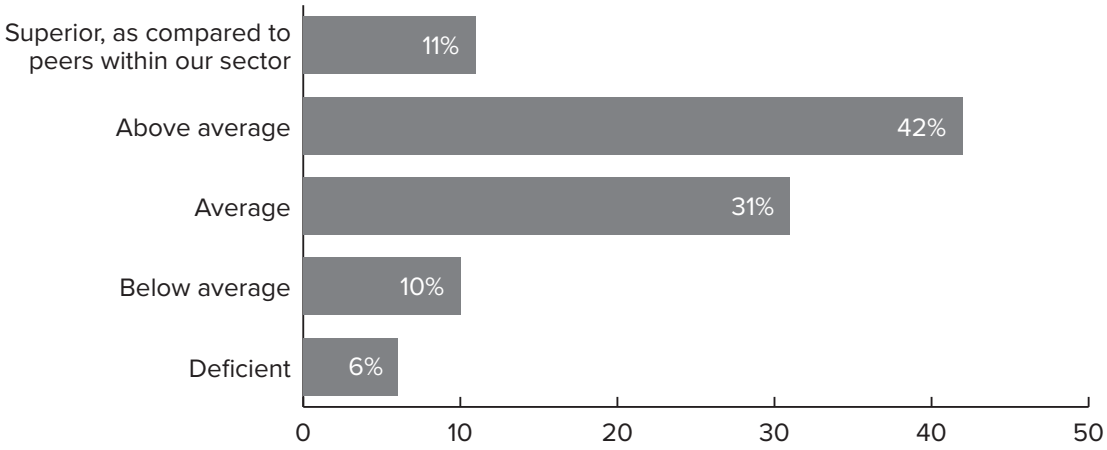
- Isolate and shut down offending systems and accounts, recover encrypted files from backups, mitigate the initial attack vector if possible – 59 percent
- Immediate in-house response: identify, contain, eradicate, recover – 27 percent

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.

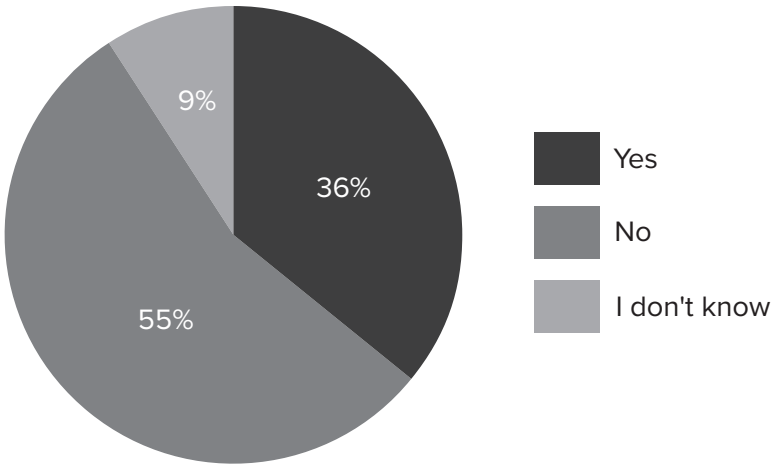
Up next: The business impact of ransomware.

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?

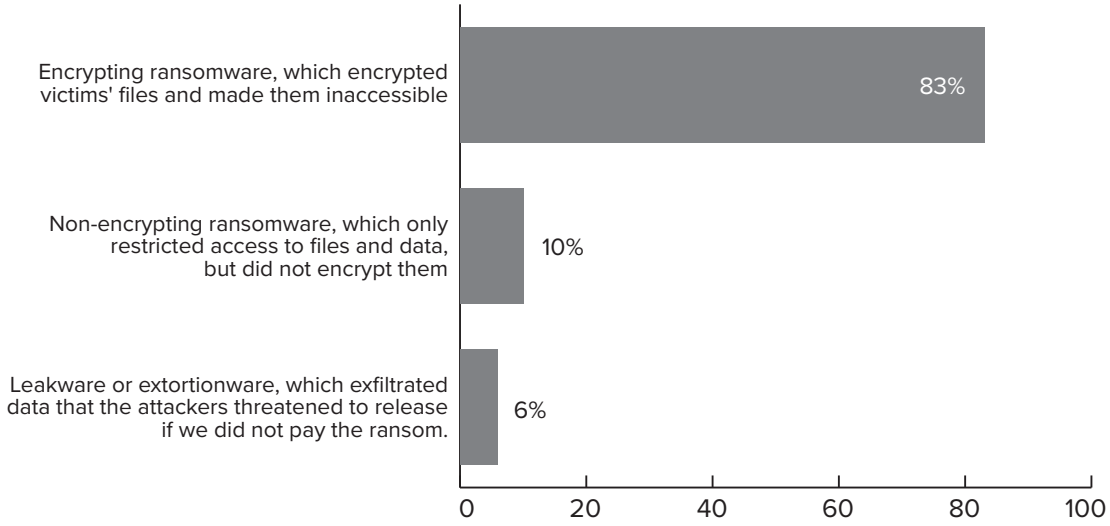


While more than half of respondents say their organizations were not ransomware victims in the past year, nearly 10 percent claim they do not know, which raises the prospect that the percentage of those who say they were victims—36 percent—could, in fact, be higher.

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.

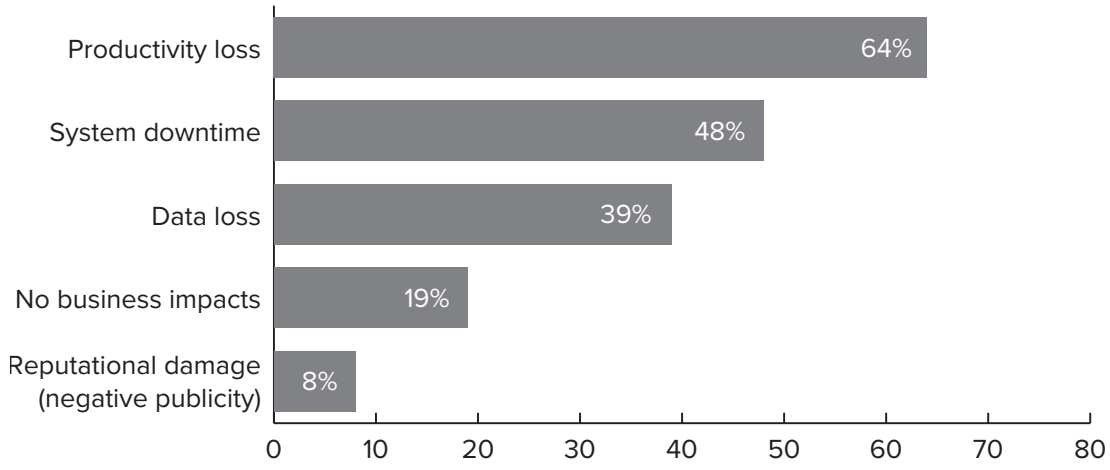
8. If you answered yes to the previous question, what type of ransomware infected your organization? (select all that apply)



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

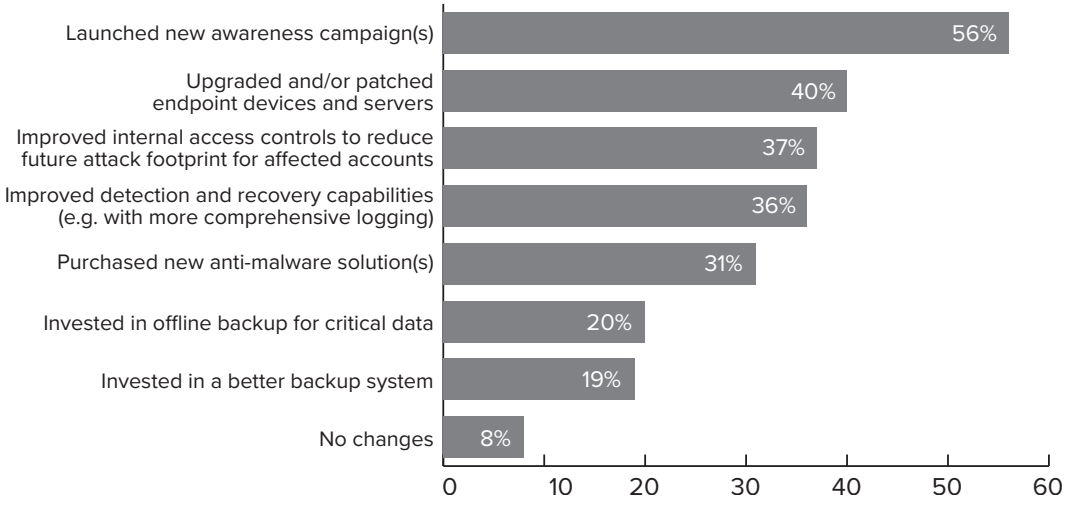
Only 10 percent report being struck by non-encrypting ransomware, which restricts access to files and data.

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)



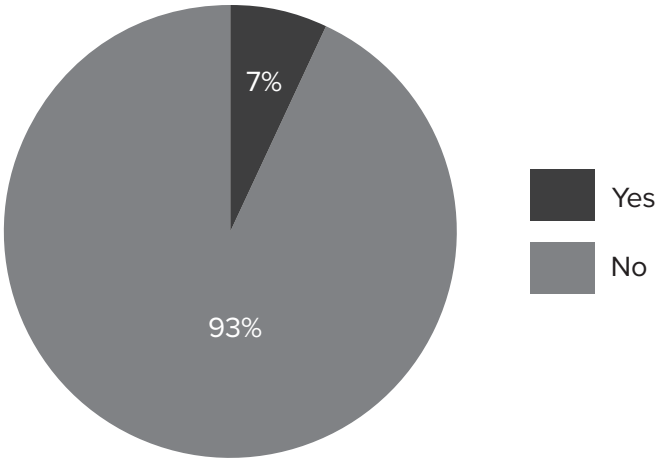
In terms of business impact, 64 percent report a productivity loss, while 48 percent say they saw system downtime, and 39 percent cite data loss.

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.”

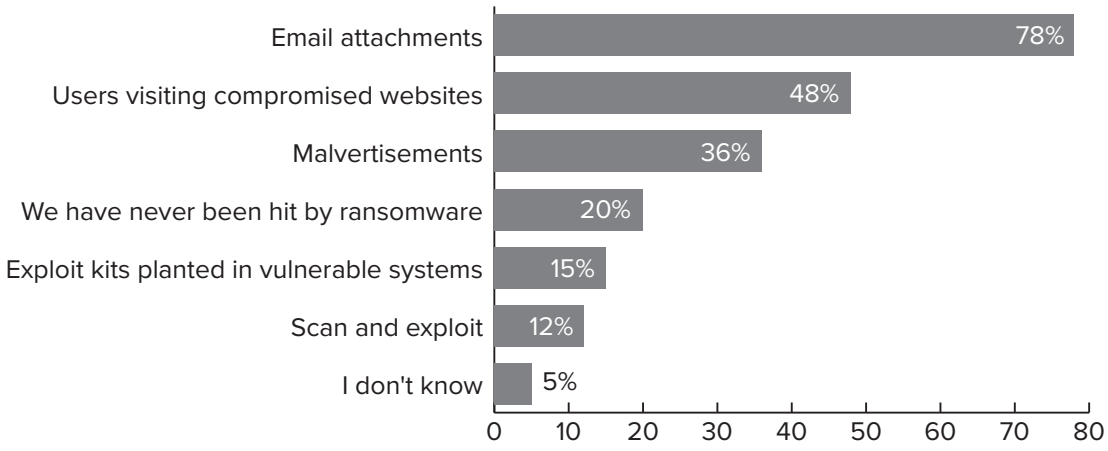
Up next: Ransomware detection.

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

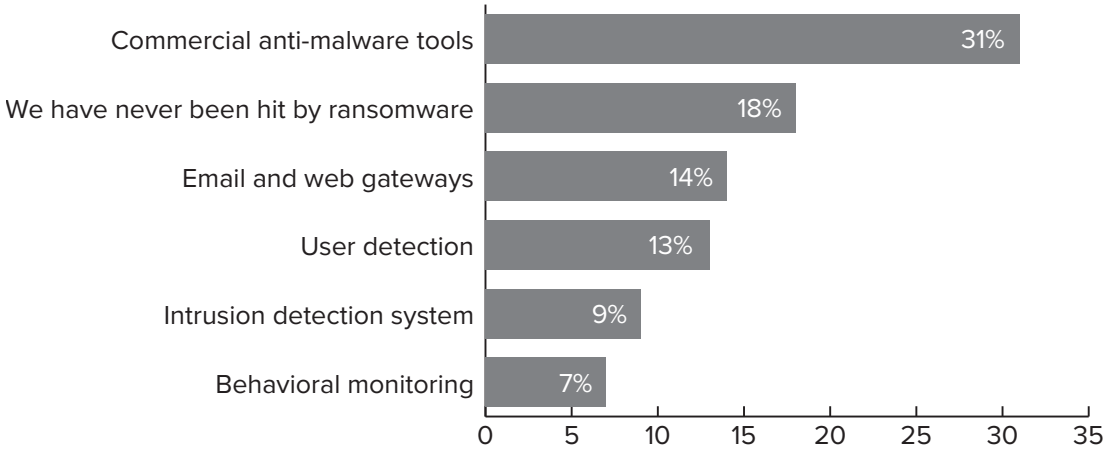
13. How does ransomware typically try to enter your organization? (select all that apply)



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).

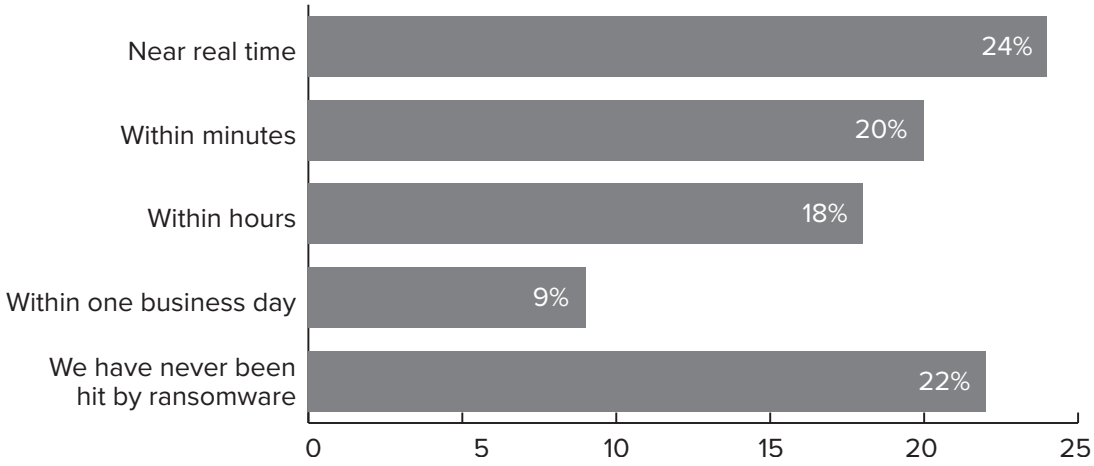
Email attachments are the most common way that ransomware typically enters organizations.

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



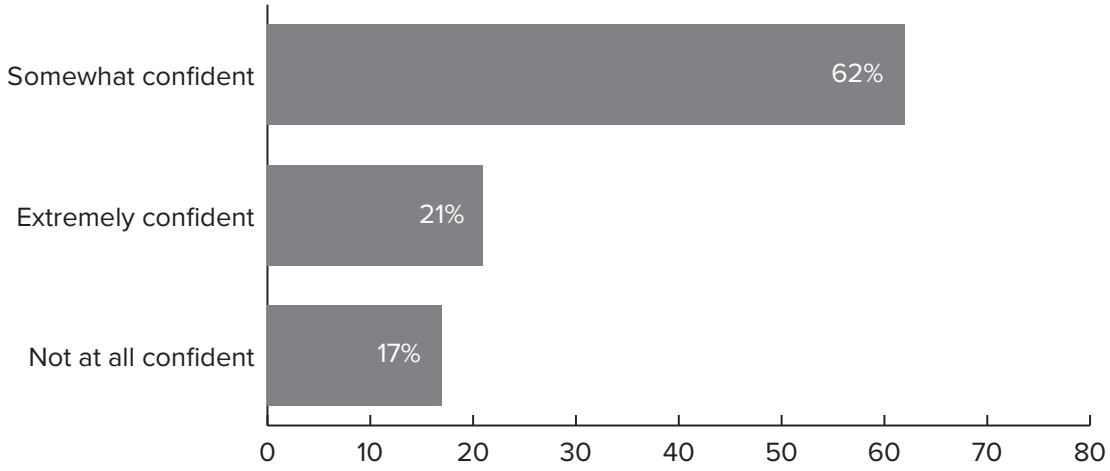
How is ransomware typically detected? The most common way is by using commercial anti-malware tools, according to 31 percent of respondents. Fourteen percent detect it via email and web gateways, while 13 percent say it is through user detection.

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.

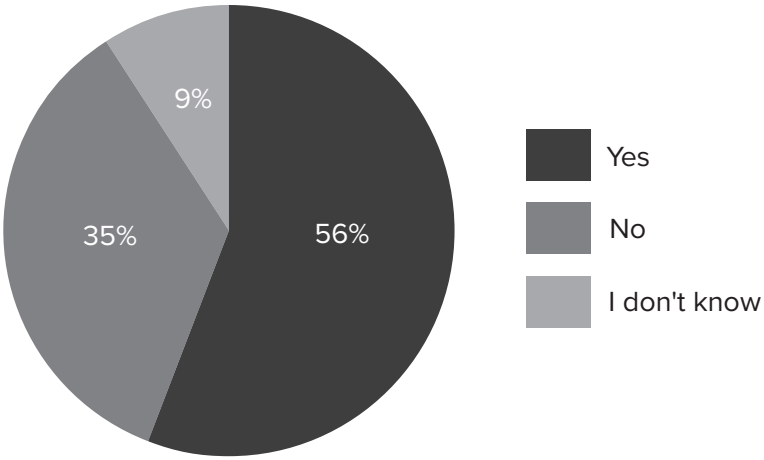
Asked about their level of confidence in the capability of their organization's defenses to detect malware on endpoint devices before it spreads from workstations and infects critical files via file-share, only 21 percent are extremely confident.

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?

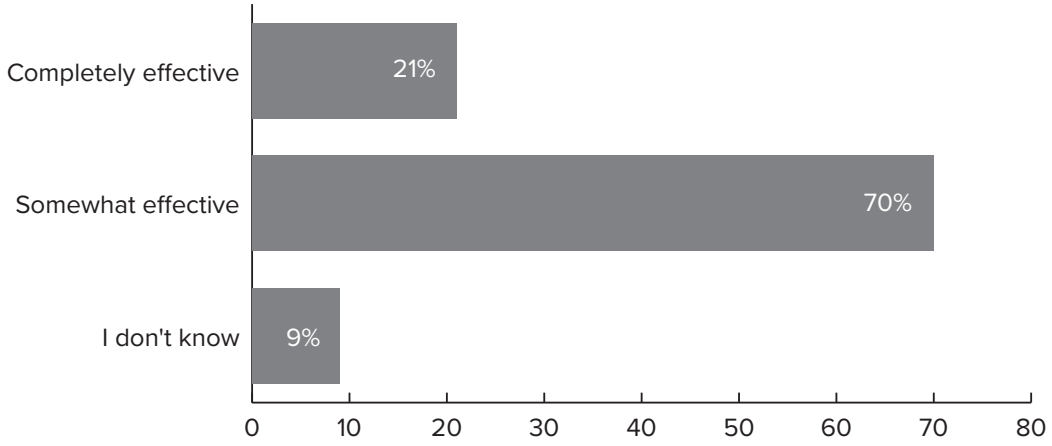


Given that three-quarters of respondents see ransomware as a significant issue, you might expect a similar response to the question: Does your organization have a ransomware response plan in place?

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.

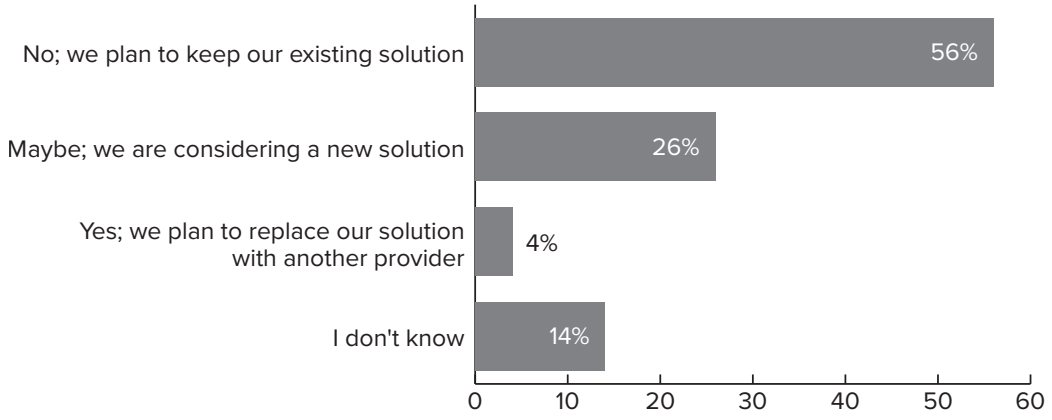
Thirty-five percent say they do not have a ransomware response plan, while 9 percent do not know.

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



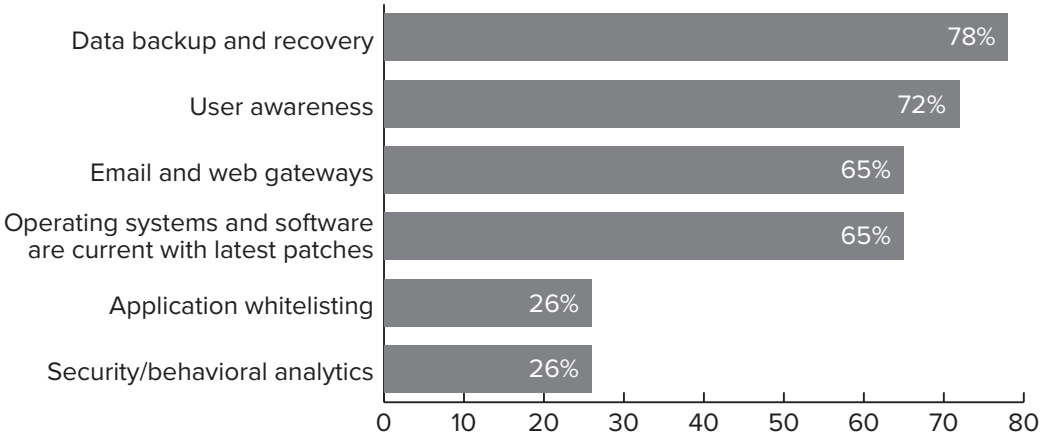
But despite the wide usage of anti-malware vendors, only 21 percent of respondents say their current solutions are completely effective at protecting organizations from ransomware. Seventy percent say the current solutions are only somewhat effective.

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? Most common responses:

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

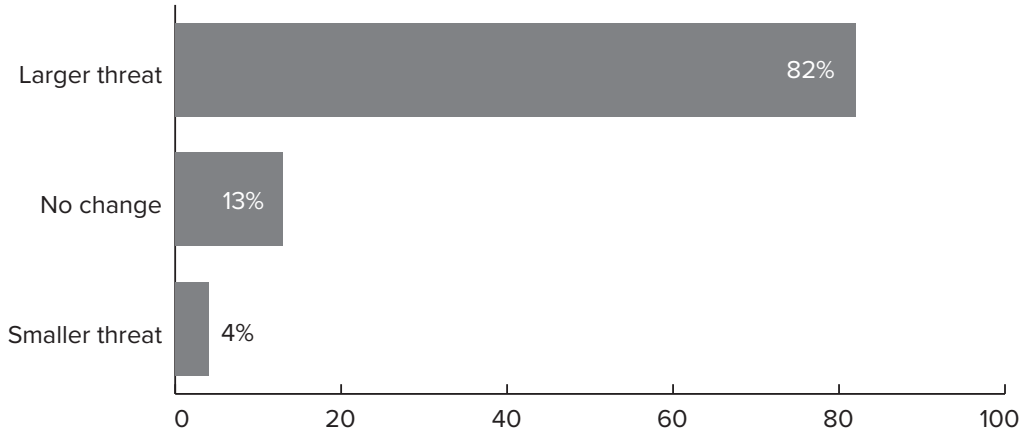
Upcoming: A look at 2017 anti-ransomware budgets and plans.

2017 Anti-Ransomware Agenda

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

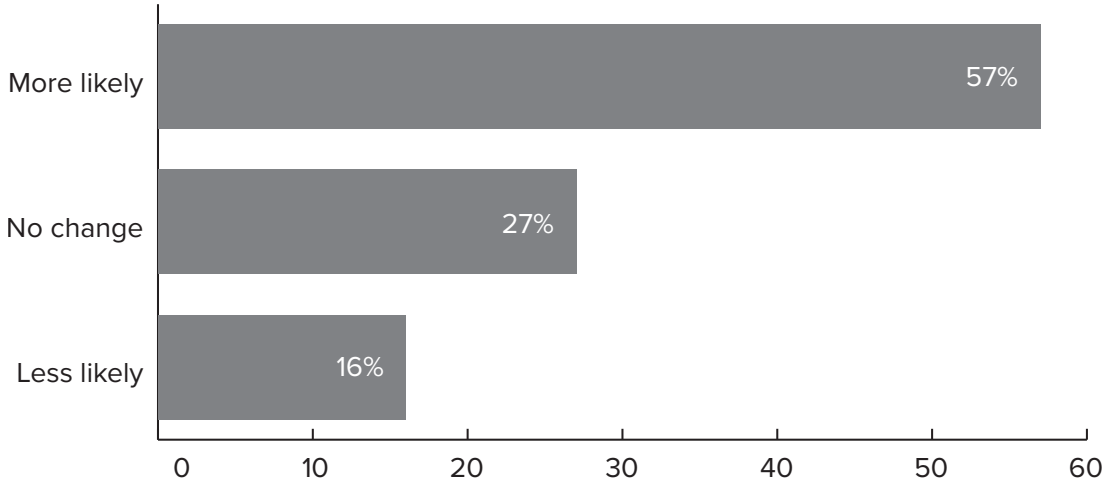
- 82 percent of respondents believe ransomware in 2017 will be a larger threat to organizations globally
- 97 percent the same or increased budget to fight ransomware

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



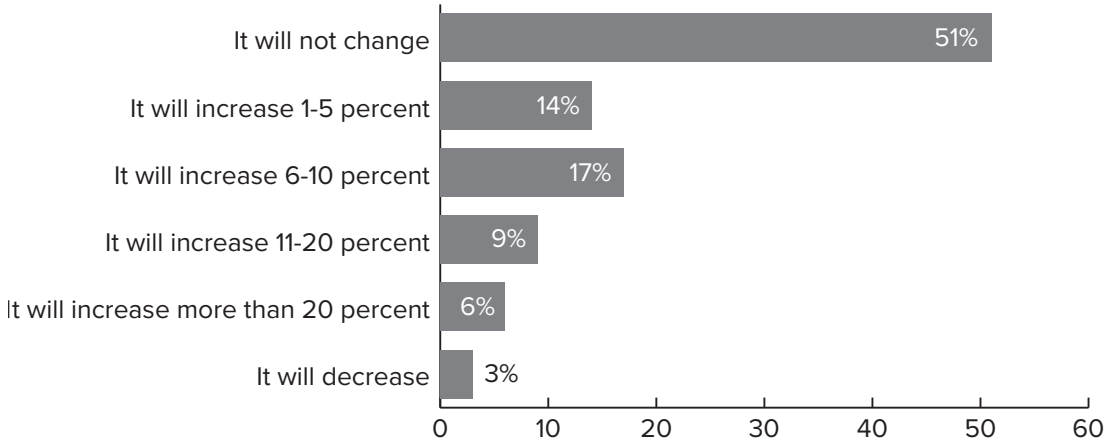
Asked whether they believe ransomware will be a larger or smaller business threat globally in 2017, only 4 percent say "smaller." The remainder see it as either a larger threat or no change from 2016.

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.

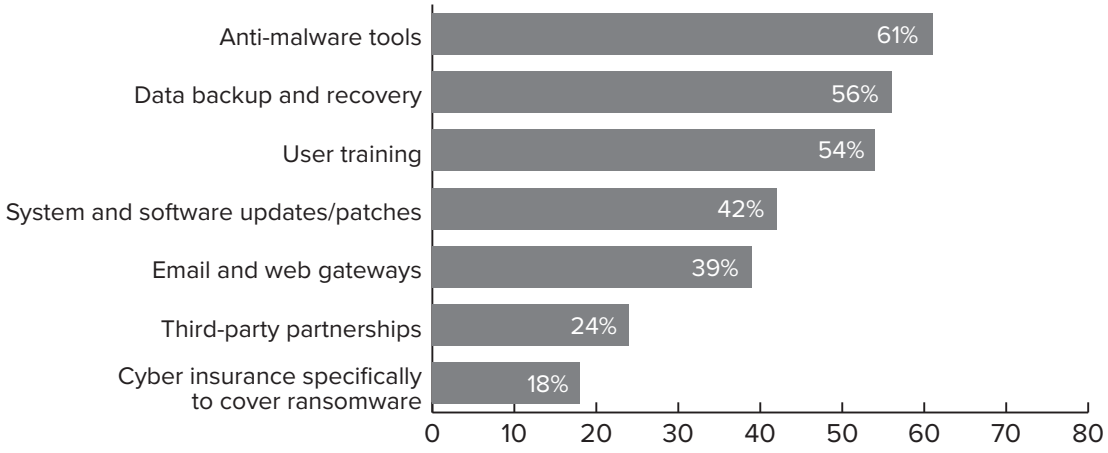
24. How do you expect your organization's budget for ransomware security to change?



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.

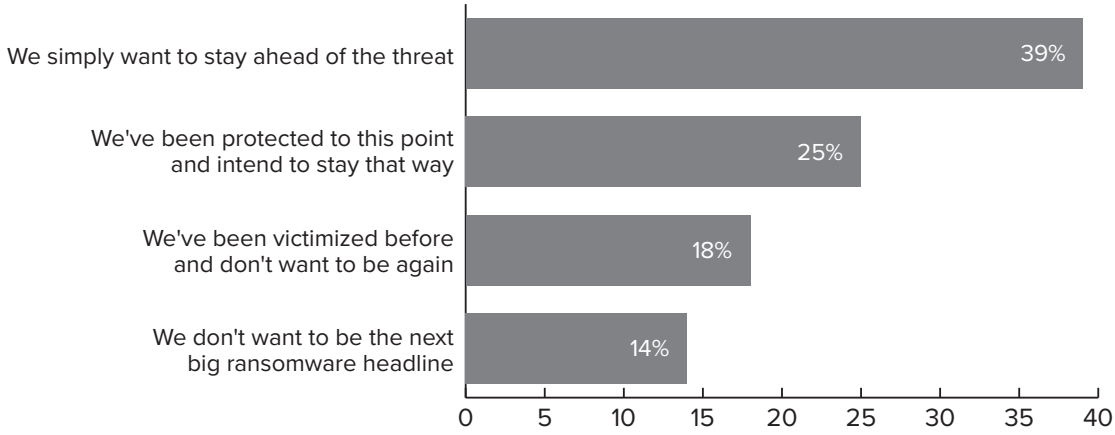
How will those funds be allocated?

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 Defense: 'What Happens if This Layer Fails?'

Survey Analysis by David Gibson of Varonis

NOTE: In preparation of this report, ISMG Vice President of Editorial Tom Field sat down with David Gibson of survey sponsor Varonis 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.

Reflections on the Results

TOM FIELD: How do you find that the overall survey results either validate or challenge some of the hypotheses you had going into the research?

DAVID GIBSON: Overall, the survey results are in line with what we thought. They show that while respondents may be worried about ransomware as a whole, they don't seem worried about themselves in particular. In other words, there seems to be a bit of a mismatch between their perceptions of the threat overall and their perception of the threat to themselves. It suggests they are overconfident in their abilities to detect ransomware and respond to them quickly.

FIELD: Did any of the responses surprise you in any way?

GIBSON: One in particular pops out. Only 14 percent of respondents agreed that enterprises must assume that malware, including ransomware, is already within their perimeters. Given that so many people have been hit with ransomware, it should be clear that it's fairly easy to get inside a perimeter.

Also, I found it interesting that 74 percent of respondents thought professional criminals capable of creating sophisticated new variants were among the primary causes of ransomware. There are 100,000 new ransomware infections a day. Ransomware-as-a-service is readily available on the dark web. It should be a logical conclusion that you don't need to be a sophisticated actor to deploy ransomware. At this point almost anybody can penetrate a network.

Finally, only 56 percent of respondents said they have a ransomware response plan in place, which includes those that have already been victims of ransomware attacks. If only slightly more than half of those surveyed have a response plan, what are the others doing? Do they really think they won't get hit again? That's weird.

David Gibson

"There seems to be a bit of a mismatch between perceptions of the threat overall and people's perceptions of the threat to themselves."

Overconfidence?

FIELD: Do organizations seem to be overconfident in their current ransomware defenses? If so, what fuels this overconfidence?

GIBSON: According to this survey, 83 percent of respondents are confident they can detect ransomware

"There are 100,000 new ransomware infections a day. Ransomware-as-a-service is readily available on the dark web. It should be a logical conclusion that you don't need to be a sophisticated actor to deploy ransomware."

at their endpoints. They don't seem to be asking themselves, "What if this layer of defense fails?" For a long time, people put their faith in their firewall and their perimeter, and now with ransomware, they're looking at their endpoints.

But how does ransomware infiltrate an organization? Typically, through a phishing attack, a hijacked website or a cloud share, bypassing that endpoint protection. They seem to be putting too much faith in endpoint protection, when they seriously need to consider other layers of defense to counter this threat.

Also, when people compare themselves with respect to their peers, they tend to overinflate some of those numbers.

Ransomware Variants

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

GIBSON: The infection points match up. As I already mentioned, phishing, hijacked websites and cloud sharing all are effective entry points for ransomware infection. At the same time, it's often hard to pinpoint exactly how ransomware gets into an organization. Therefore, you have to assume that bad actors are either already in your organization or are going to infiltrate it, and you must prepare as if that is the case.

Also fascinating, albeit not unexpected, was the percentage of respondents who said they've been hit with extortionware. I think we'll see an increase in extortionware because it potentially is more lucrative than straight ransomware. People are even more reluctant to report extortionware because that's its point: If you don't pay me, I'll leak this data and make it public.

Bolstering Defenses

FIELD: Respondents expressed to us a lack of confidence in their current anti-malware solutions to protect their organizations from ransomware. What are your recommendations on how they bolster those defenses?

GIBSON: You need to take a defense-in-depth approach. You need to look at any layer and ask yourself: "What happens if this layer fails?" In addition, you need to prioritize building layers around the assets you're most concerned with protecting. The highest concentration of data targeted in ransomware attacks usually are on your client shares. There is 10 to 1,000 times more data on a file share than on a laptop or a workstation. So, putting a ring around your crown jewels just makes good sense.

The User Problem

FIELD: It's become cliché to say this, but users are the weak link in the security chain and can cause serious business disruption. How then do you advise security leaders to address this issue with users, because clearly past efforts have not been effective?

GIBSON: Fifty-six percent said they were launching new awareness campaigns, and I hope to see that number grow. Security leaders need to illustrate recovery costs but also productivity costs that happen when you are unable to access your intellectual property and can't work.

This awareness is greater in healthcare because if a healthcare entity is forced to shut down and can't serve patients, lives can be lost. The impact is stark.

Ransomware Trends to Watch

FIELD: As we enter 2017, what ransomware trends are you observing?

GIBSON: If you go to Google trends, you'll see that the searches for ransomware start spiking in Q1 of 2015. While there have been a few dips, it keeps coming back to that same level—which suggests to me is that people are still learning about ransomware.

But what I don't see happening is the notion that these attacks are the canary in the coal mine. The vulnerabilities exploited by ransomware have been around for over

10 years, and people have had way more access to the data inside their organization than they should have for a long time. I saw a recent survey that said 64 percent of end users say they have access to much more data than they need to do their job. Another compounding factor is that organizations are not monitoring how people inside the network are using information such as file shares or emails. If you run a bank and everybody inside the bank can get into the vault and you weren't watching what people are taking out of the vault, what's going to happen?

It should be a wake-up call that the vulnerabilities that ransomware exploits beyond the endpoint must be addressed because even if they don't lead to ransomware attacks, they can lead to something else. So, people need to address these vulnerabilities, and I hope they themselves start to make that conclusion.

Investing Resources

FIELD: What first steps should security leaders do to shore up their ransomware defenses?

GIBSON: Following up on the previous question, assess your assets, starting with your most valuable data. Where is it? Who has access to it? Who is using it? What does normal usage look like? Is any of your data exposed to too many people—and how do you control user access? Could your organization lock down, or even dispose of, any of that data, given the regulatory environment?

Then set up credentials using the principle of least privilege. By limiting access, you have better visibility when supposedly trusted users abuse their privilege or their account gets hijacked.

Final Advice

FIELD: What's your final advice for organizations seeking to improve their overall ransomware defense?

GIBSON: It's always best to respond to threats before they happen. So, ask yourself this question: "What happens when a bad actor enters our network?"

Do a tabletop exercise. Talk it through. If the files get encrypted on the endpoint and the workstation and it doesn't get picked up and then the ransomware goes out and starts to encrypt data on file shares, what is going to detect that and when? How will you respond? Can you see exactly which files were encrypted?

Walking through each of the different threats is critical to responding to not just ransomware, but also other threats that come your way in the future. ■

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