2016

RANSOMWARE RESPONSE STUDY

What is *Your* Organization Prepared to Do When the Extortionists Come Calling?

INSIDE:

- Complete Survey Results
- Expert Analysis
- Insights from Eduardo Cabrera of Trend Micro

TREND MICRO™

ISMG INFORMATION SECURITY MEDIA GROUP

Tom Field
Vice President, Editorial

About the Ransomware Response Study

Fifty-nine percent of security leaders believe their current ransomware defenses are above average or superior. And yet 53 percent also say they have been victim of ransomware attacks in the past year.

This is but one of the preliminary results of the 2016 Ransomware Response Study.

Reviewing the total 225+ responses to this survey, the results show heightened awareness to the ransomware threat: 54 percent of respondents have discussed ransomware with their boards, and 61 percent say their organization's ransomware awareness is above average or superior.

These are among the results of the 2016 Ransomware Response Study.

Aimed at determining how prepared organizations are for a ransomware attack, the survey finds that their biggest vulnerability is the susceptibility of their own employees. And while 77 percent say they have never paid ransom in response to such an attack, 54 percent also say that although paying ransom is generally a bad idea, sometimes it's the easiest way to restore business.

There is good news in the survey results, too: 98 percent of respondents expect the same or increased budget to fight ransomware in the year ahead. What are their top spending priorities? Read on to learn more. And pay special attention to our exclusive survey analysis at the end of this report, where we offer expert insight on how to best put these survey results to work to protect your organization from the ransomware scourge.

Best,

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

This survey was conducted online in the summer of 2016, and it generated more than 225 responses from organizations across industrial sectors in the U.S. Among those respondents, 27 percent were from government, 28 percent were from healthcare, and 38 percent were from financial services. Generally, the survey results were very consistent across industry sectors. But in a few key areas, there were significant distinctions, and those will be highlighted where appropriate in this report.

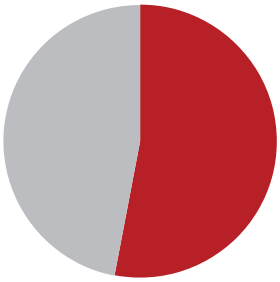
About Trend Micro:

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud.

For more information, visit www.trendmicro.com.

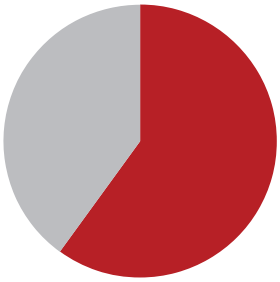
By the Numbers

Some statistics that jump out from this study:



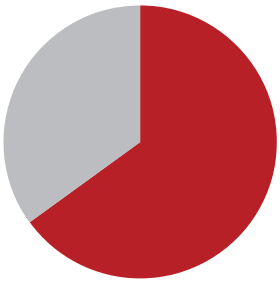
53%

of respondents have been a victim of ransomware attacks in the past year.



60%

say their biggest vulnerability is the susceptibility of their own employees.



65%

say ransomware is most frequently encountered when users visit compromised or bogus sites.

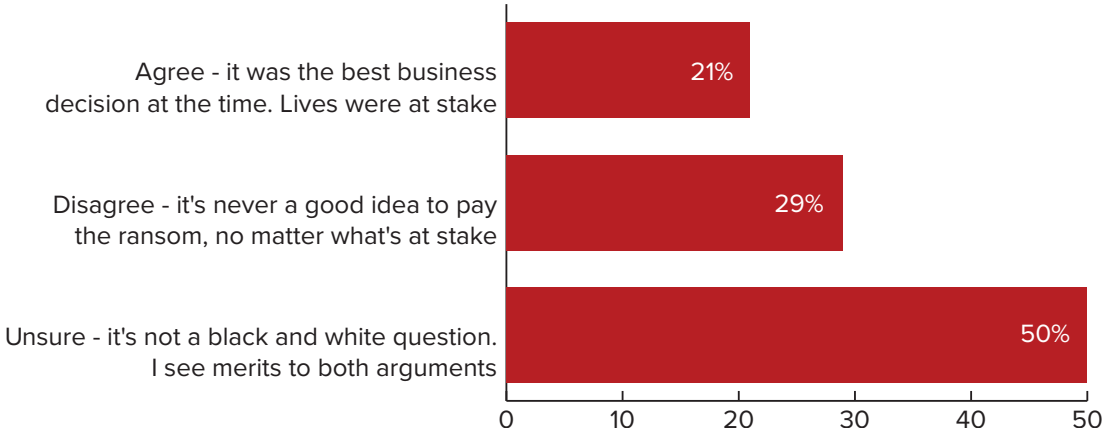
Baseline Ransomware Questions

In this opening section, the report establishes some of the fundamental views on ransomware and how it's taken root in organizations. Among the key findings:

- 53 percent of respondents have been ransomware victims in the past year.
- 59 percent have suffered business disruption resulting from those attacks.

Read on for full scene-setting results.

Earlier this year, Hollywood Presbyterian Medical Center made news for paying $17,000 to end a ransomware attack. Do you agree or disagree with the hospital's decision?



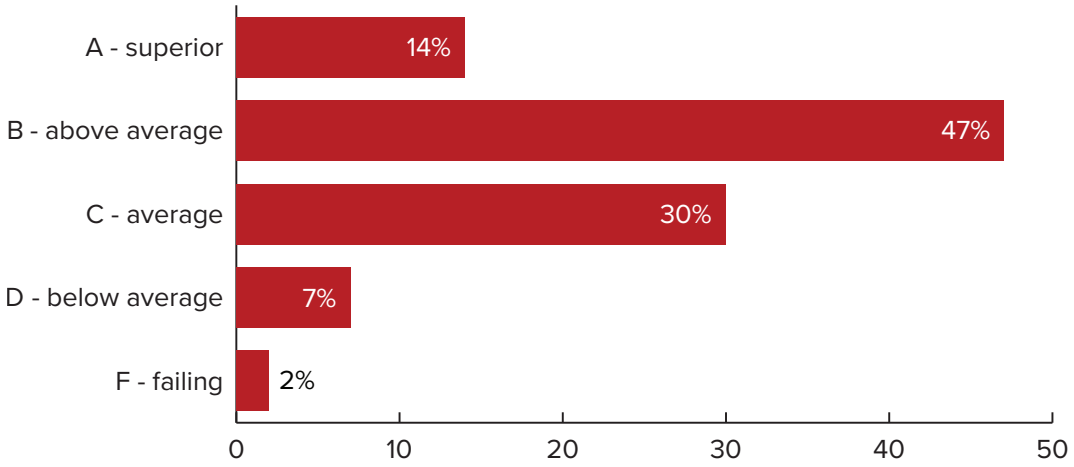
Fair or no, Hollywood Presbyterian has become the poster organization for ransomware. Its high-profile response to an attack–paying the ransom–has been discussed worldwide throughout the year.

How many people agree with the hospital's controversial decision? According to the survey results, only 21 percent of respondents openly agree. Twenty-nine percent say they absolutely disagree.

But the telling statistic: An even 50 percent say this is not a simple, black and white question. They see merits in both sides of the argument.

How many people agree with [Hollywood Presbyterian's] controversial decision? According to the survey results, only 21 percent of respondents openly agree. Twenty-nine percent say they absolutely disagree.

In light of recent high-profile attacks, how do you assess your organization's level of awareness to the ransomware threat?



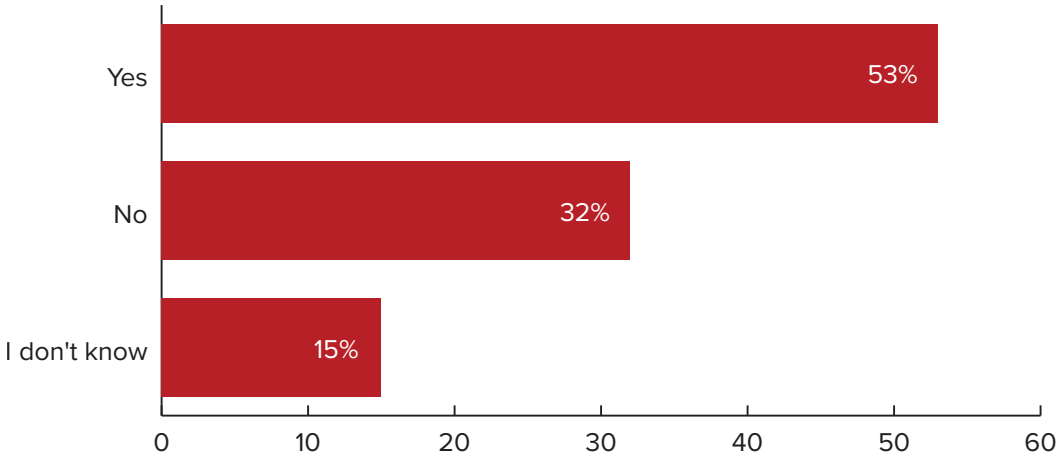
Given the prevalence of high-profile attacks such as the one that struck Hollywood Presbyterian, ransomware has become a boardroom conversation. Many a security leader has been taken aside and asked "Are we protected?"

How, then, do survey respondents rate their own organization's level of awareness to the ransomware threat?

Sixty-one percent rate awareness levels at above average or superior. Only nine percent rate themselves at below average or failing.

Yet, awareness alone has not been enough to protect these organizations. See the next chart.

Has your organization in the past year fallen victim to ransomware (systems locked or data encrypted)?

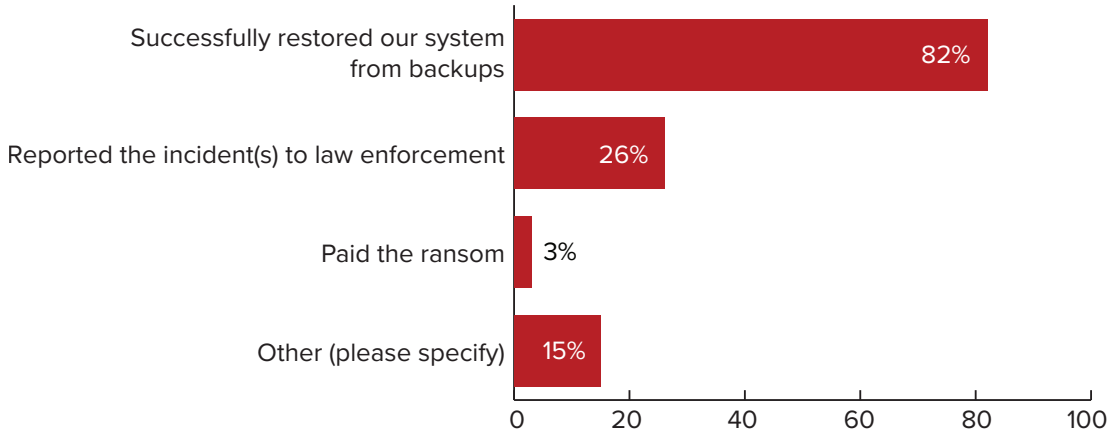


Despite high levels of awareness, 53 percent of respondents say their organizations have been victims of ransomware attacks in the past year. Only 32 percent say they have not been attacked, while 15 percent are uncertain.

Industry breakout: Interestingly, only 33 percent of financial organizations say they suffered ransomware attacks in the past year. But among government respondents, 67 percent suffered attacks.

How did organizations across sectors respond to these attacks?

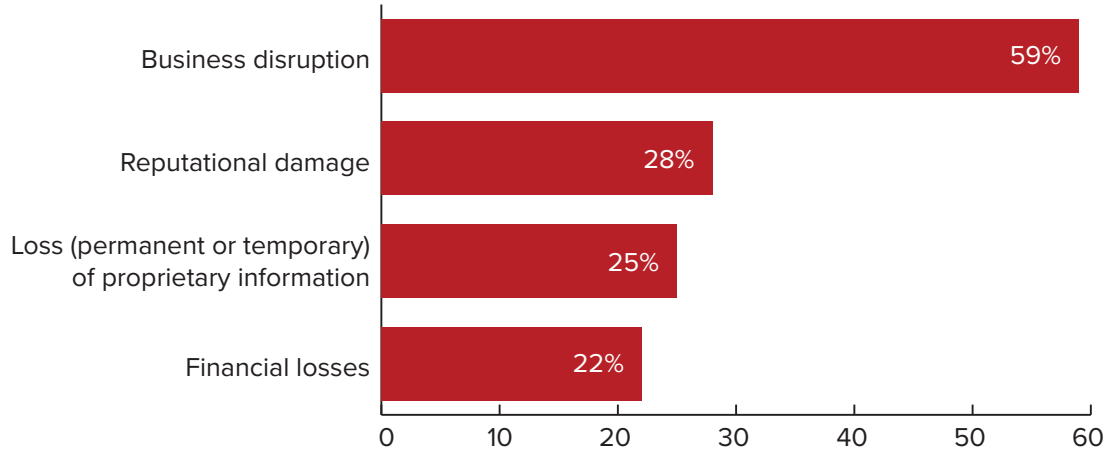
If you answered yes to the previous question, how did your organization respond to the successful ransomware attack(s)? (select all that apply)



Eighty-two percent say they took the textbook response to ransomware–they successfully restored their systems from backups. Just over one quarter say they immediately reported the incidents to law enforcement.

Meanwhile, only three percent said they surrendered to demands and just paid the ransom.

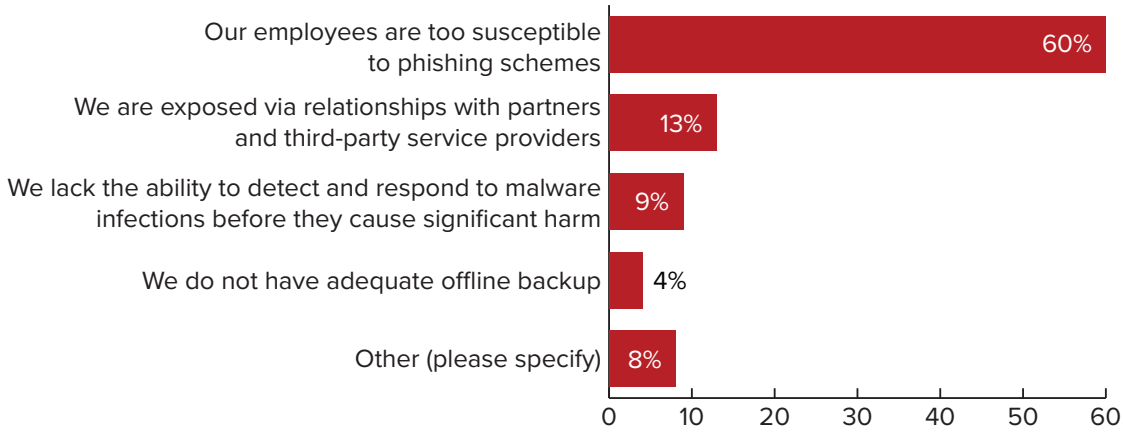
What consequences has your organization felt as a result of ransomware infections? (select all that apply)



For those organizations struck by ransomware, what are the biggest consequences they have felt?

Fifty-nine percent say they have suffered business disruption. Twenty-eight percent report reputational damage (presumably from the unwanted publicity), and 25 percent say they have suffered loss–permanent or temporary–of proprietary data.

What do you believe to be your organization's biggest vulnerability to ransomware attacks?



Asked to name their biggest vulnerability to ransomware attacks, 60 percent of respondents say it's their own employees. They are too susceptible to the phishing schemes that often deliver such payloads.

Thirteen percent say their chief vulnerability is a result of third-party risks.

In the next section, the report takes a deeper look into the specifics of ransomware attacks.

Asked to name their biggest vulnerability to ransomware attacks, 60 percent of respondents say it's their own employees. They are too susceptible to the phishing schemes that often deliver such payloads.

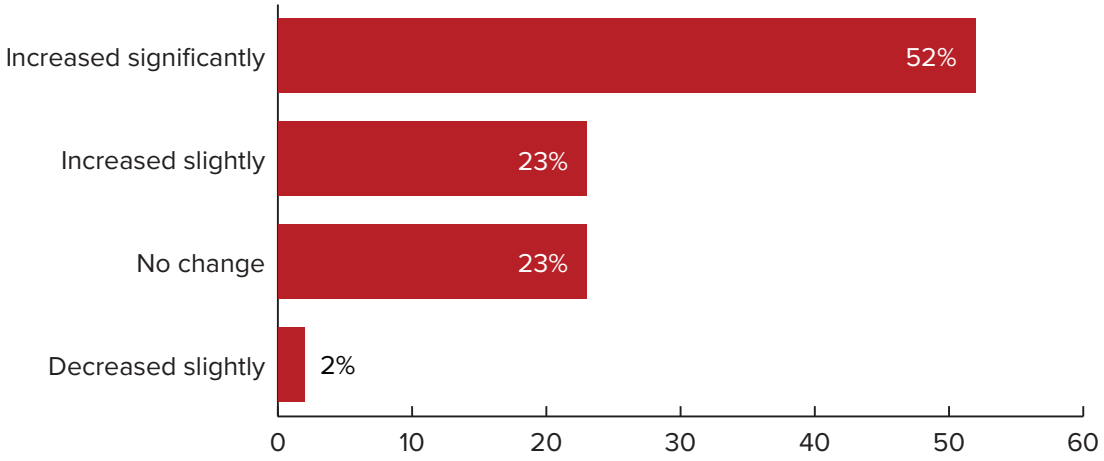
Ransomware Attacks

This section of the report delves into some of the specifics of ransomware attacks–how frequently they occur and how they are delivered. Among the takeaways:

- 19 percent of respondents say their organizations are attacked more than 50 times per month.
- 65 percent say the most common source of infection is when users visit compromised or bogus websites.

The full results follow.

How has the pace of ransomware attacks changed over the past year?



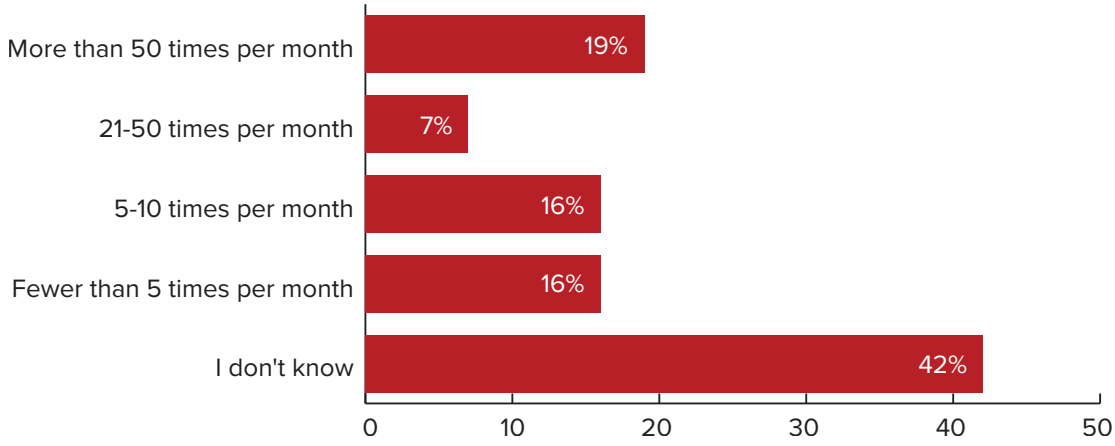
No disputing this: Ransomware isn't new to the threat landscape, but it certainly has increased its footprint in the past year.

Seventy-seven percent of respondents declare some level of increase in the pace of attacks, while 23 percent say it has stayed the same as last year. Only two percent report a slight decrease.

Industry breakout: No surprise. Although 52 percent of all organizations say they have seen a significant uptick in ransomware attacks, that number is 66 percent for healthcare where high-profile attacks have been reported widely. Overall, 85 percent of healthcare organizations say they have seen some increase in ransomware attacks.

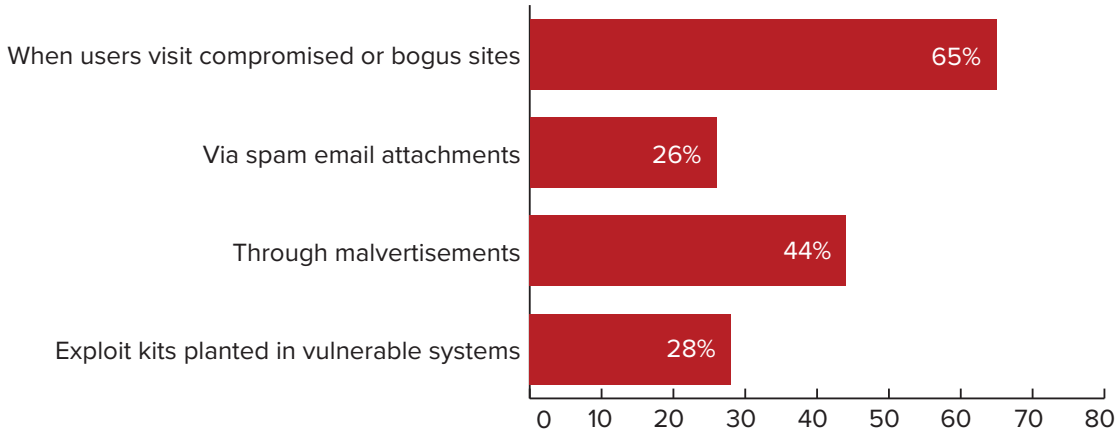
Although 52 percent of all organizations say they have seen a significant uptick in ransomware attacks, that number is 66 percent for healthcare where high-profile attacks have been reported widely.

How frequently do you believe attackers attempt to strike your organization with ransomware?



Many respondents (42 percent) do not know how frequently ransomware attackers attempt to strike their organizations. But among the majority who do, 19 percent say it is more than 50 times per month. Meanwhile, 16 percent say the pace is 5-10 times per month, while 15 percent say the number is fewer than five.

How is ransomware typically delivered to your organization? (select all that apply)



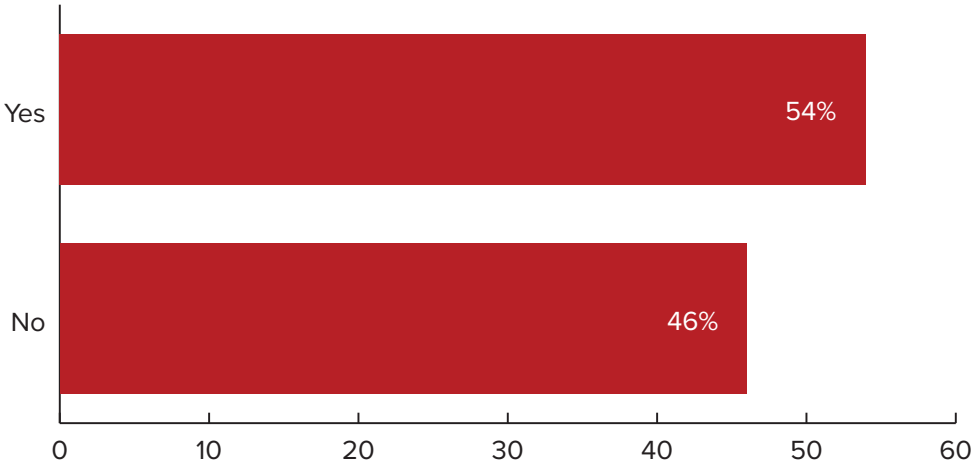
It is commonly believed that ransomware attacks are delivered primarily via spam email attachments to unsuspecting users. But, according to survey respondents, that is only the fourth most common form of infection (at 26 percent). The top three selections are:

- When users visit compromised or bogus sites – 65 percent
- Through malvertisements – 44 percent
- Exploit kits planted in vulnerable systems – 28 percent

Industry breakout: The primary methods of infection do differ across industries. The survey finds:

- Financial services – 80 percent see attacks primarily via email attachments.
- Healthcare – 67 percent also see attacks primarily via email attachments.

In the past 12 months, have you briefed your board on the operational risk ransomware presents to your enterprise?



How much of a board-level issue is ransomware today?

Fifty-four percent of respondents say they have briefed their boards on the operational risk posed by ransomware. Forty-six percent say they have not done so–yet.

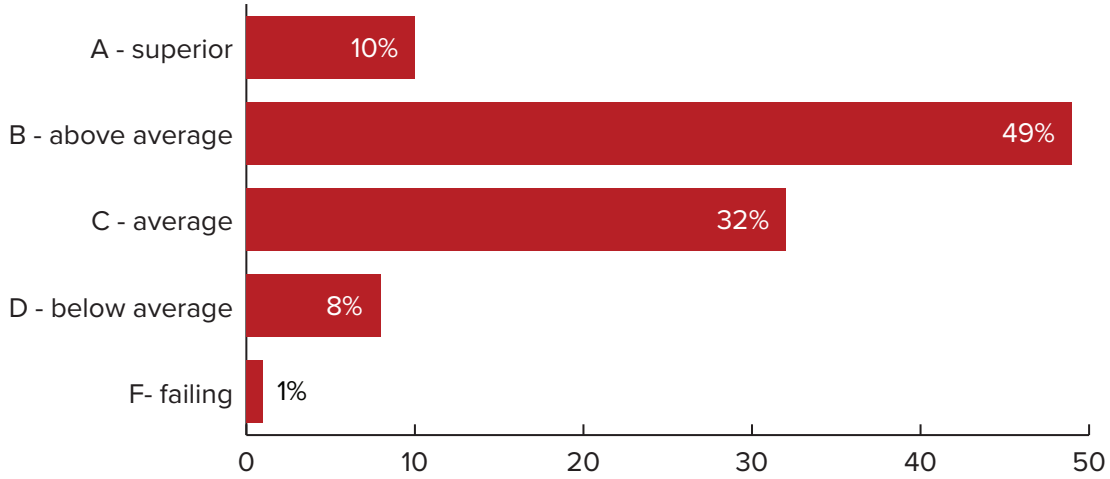
The next section of the report dives into responses related to ransomware defenses.

Ransomware Defense

In this section, the report looks at fundamental ransomware defense–how organizations assess their defenses, as well as which tools they are deploying on the front lines. Among the standout statistics:

- 59 percent of respondents assess their current defensive abilities at above average or superior.
- 78 percent say their primary defense is a data backup and recovery plan.

How do you assess your organization's current ability to defend against ransomware attacks?



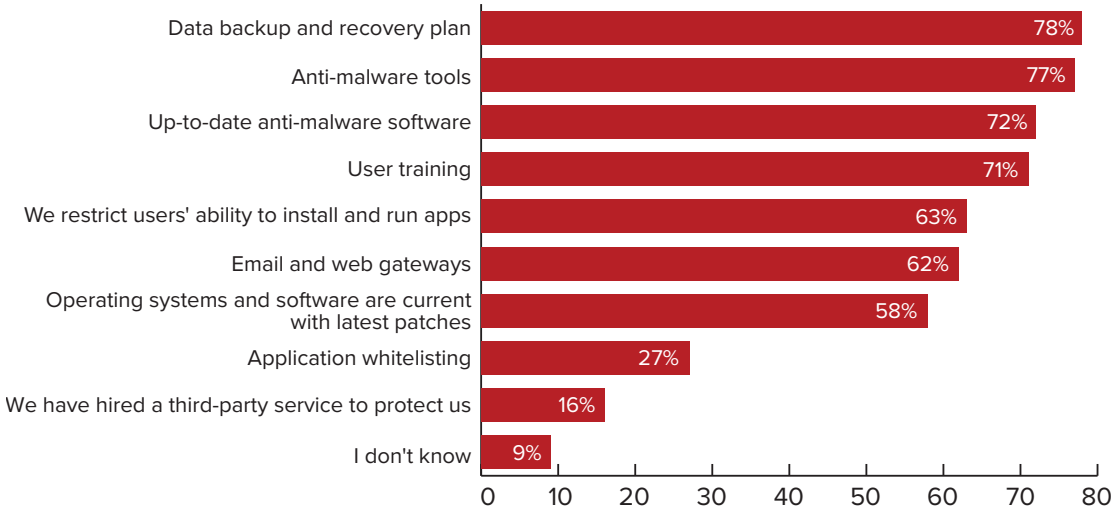
In contrast to the 53 percent of respondents who say they have been struck by ransomware attacks this year, 59 percent rate their organizations' defensive abilities at above average or superior.

Only nine percent rate their defenses at below average or failing.

What, then, are organizations deploying for defense?

In contrast to the 53 percent of respondents who say they have been struck by ransomware attacks this year, 59 percent rate their organizations' defensive abilities at above average or superior.

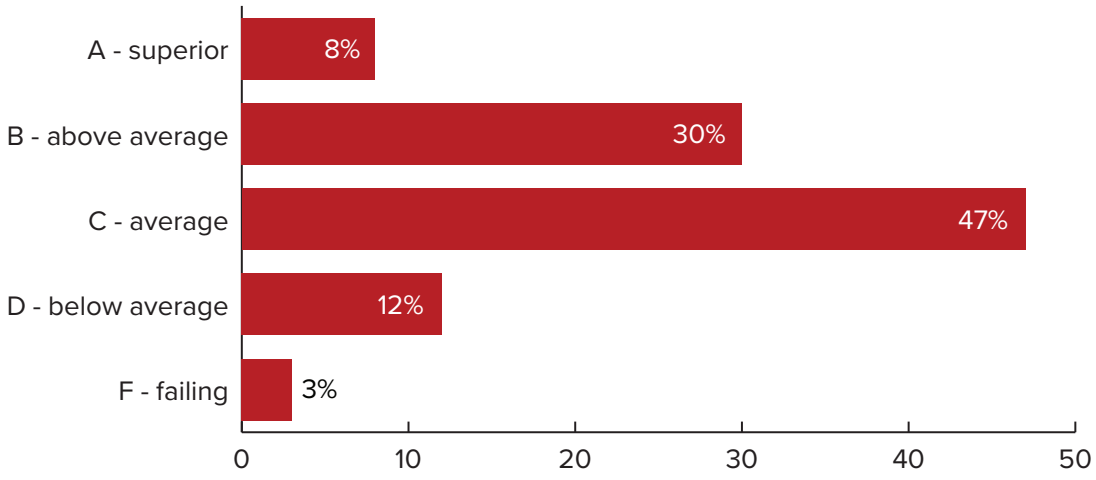
What are your primary defenses against ransomware? (select all that apply)



"Backups, backups, backups" is the common refrain given as advice to organizations to avoid being disrupted by ransomware. And, indeed, 78 percent of respondents say data backup and recovery plans are their primary defense. Other top responses:

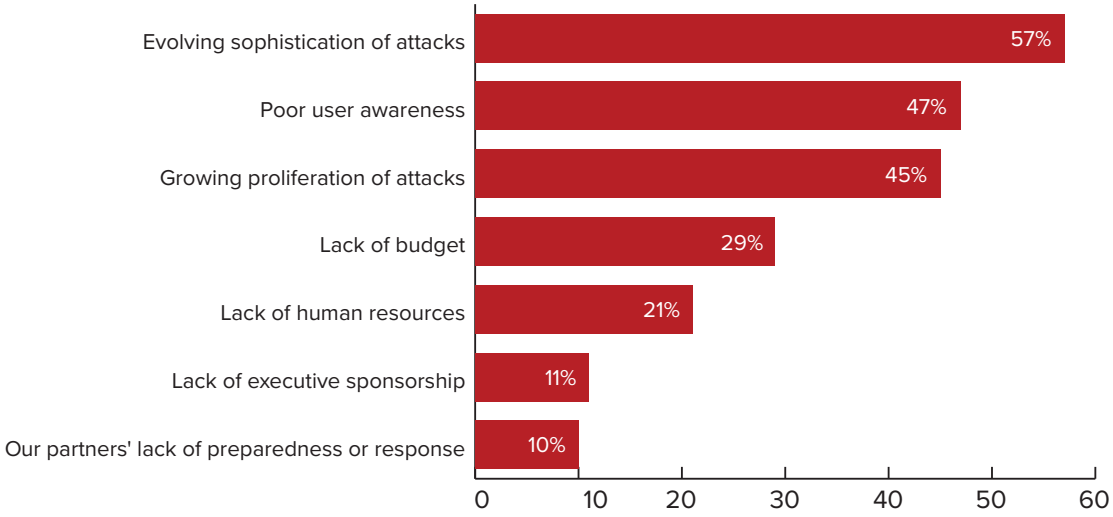
- Anti-malware tools – 77 percent
- User training – 71 percent
- Email and web gateways – 62 percent

How do you assess your organization's level of user awareness to defend against ransomware attacks?



Security leaders often bemoan the lack of user awareness to threats such as ransomware. And, in fact, 62 percent of respondents assess their organizations' levels of user awareness to be average at best. Only eight percent rate their user awareness as superior.

What do you believe to be your organization's biggest obstacles to improving ransomware defense? (select all that apply)



No surprise, then, that 47 percent of respondents say "poor user awareness" is among their biggest obstacles to improving ransomware defense. Rounding out the top three responses: Evolving sophistication of attacks (57 percent) and growing proliferation of attacks (45 percent).

Next, the report explores how organizations respond to ransomware when they are attacked.

47 percent of respondents say "poor user awareness" is among their biggest obstacles to improving ransomware defense.

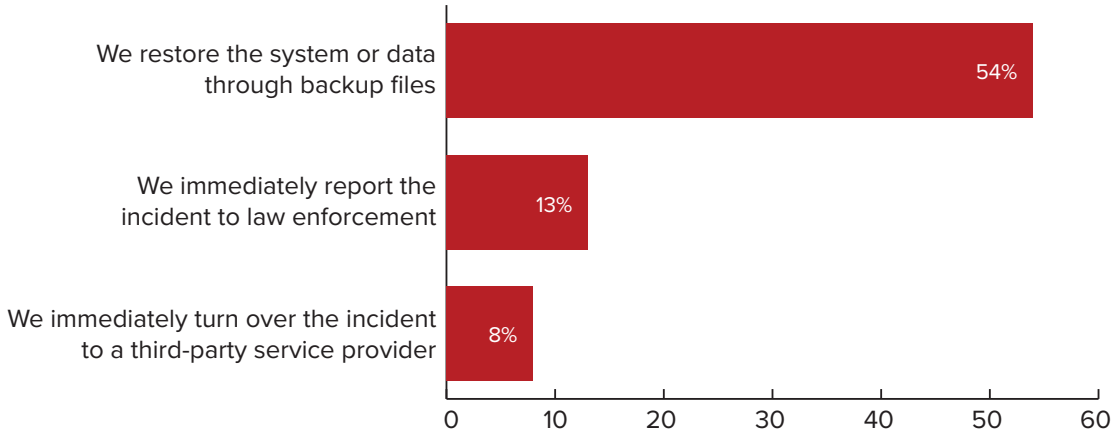
Ransomware Response

What *do* organizations do when they find they have been struck by ransomware?

- 54 percent say they immediately restore the system through backup data files.

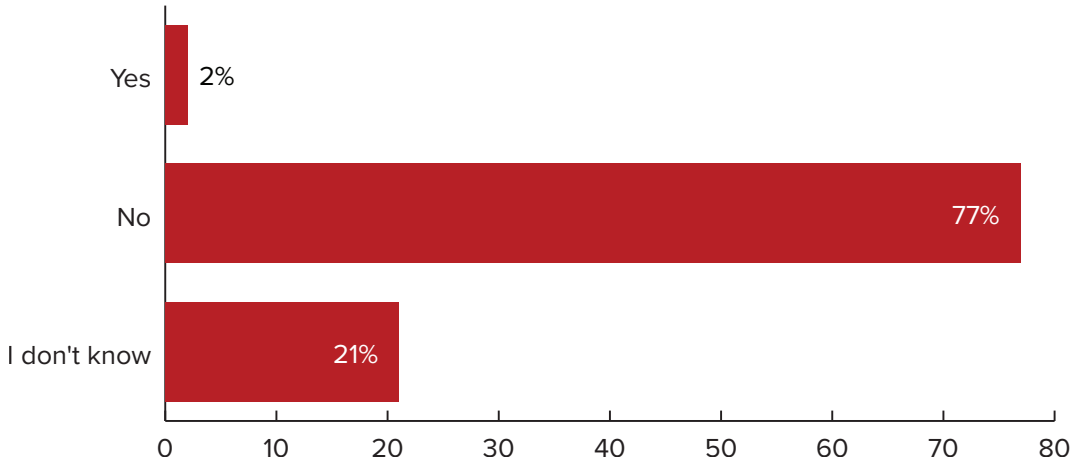
The following charts depict other aspects of response strategies.

What is your organization's primary response to a successful ransomware attack?



Security leaders are often told to report ransomware attacks immediately to law enforcement. But only 13 percent of respondents say that is their approach. The majority–54 percent–say they restore systems through backup files.

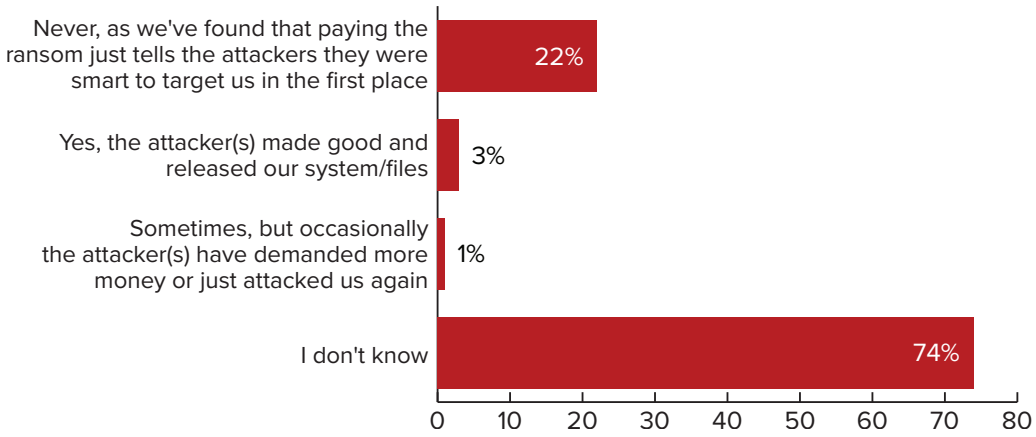
Has your organization ever paid ransom as a result of a ransomware attack?



The big question: Have you ever paid ransom as a result of a ransomware attack?

Seventy-seven percent of respondents say absolutely “no.” Only two percent acknowledge they have, while 21 percent are uncertain.

If your organization *has* paid ransom, has that successfully ended the attack(s)?

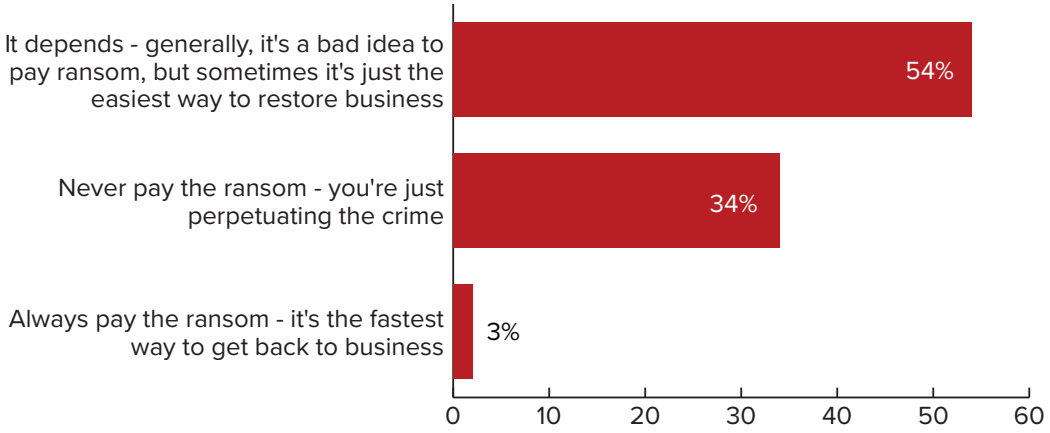


One of the arguments against paying ransom is that it reinforces the attackers were right to target you in the first place and does not guarantee the attack will end.

Seventy-four percent do not know whether paying ransom did, in fact, end the attacks.

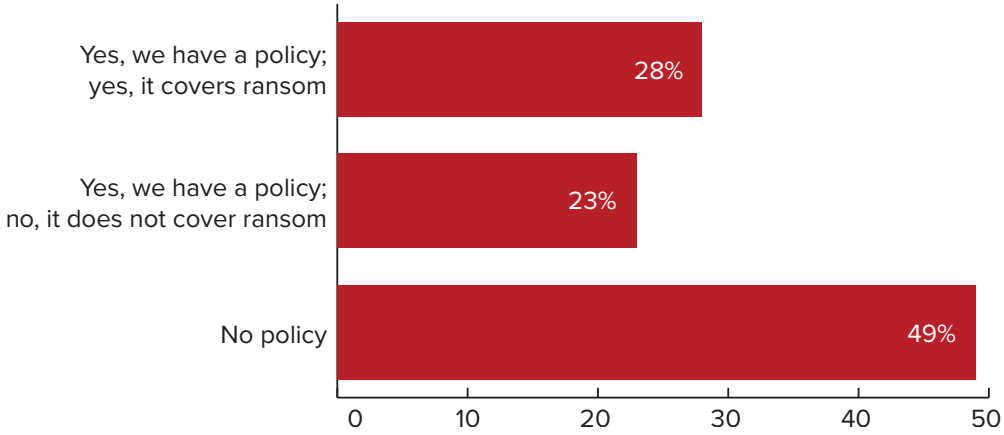
Meanwhile, 22 percent say they have found that "paying the ransom just tells the attackers they were smart to target us in the first place."

What advice would you offer to other organizations re: paying ransom to attackers?



As for the advice they would offer other organizations re: ransom, 34 percent say, "Never pay the ransom," while 54 percent say, "It depends." The logic is: Paying up is never a good idea, but sometimes it is the easiest way to restore business.

Does your organization have a cyber insurance policy, and does it cover ransom requests?



Increasingly, cyber insurance providers have strong say about the components of an organization's cybersecurity defenses. But 49 percent of respondents say they do not have such a policy. Of those that do, 28 percent say the policy covers ransomware; 23 percent say it does not.

Industry breakout: There are some differences by industry re: cyber insurance. For instance, 78 percent of financial services respondents say their organizations do have cyber insurance. And 46 percent say these policies do not cover ransomware.

In contrast, 63 percent of healthcare entities say their have cyber insurance, and 43 percent say their policies do cover ransomware.

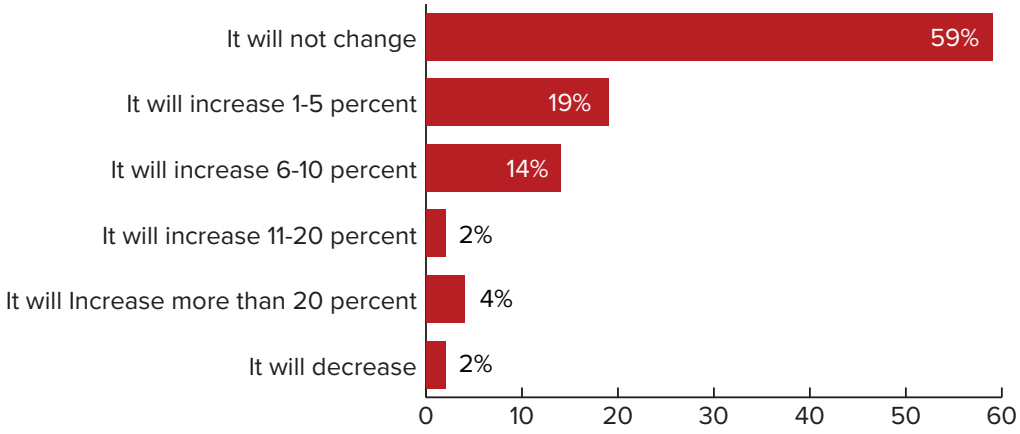
Next, the report looks at anti-ransomware resources and plans for 2017.

Increasingly, cyber insurance providers have strong say about the components of an organization's cybersecurity defenses. But 49 percent of respondents say they do not have such a policy.

Ransomware Resources

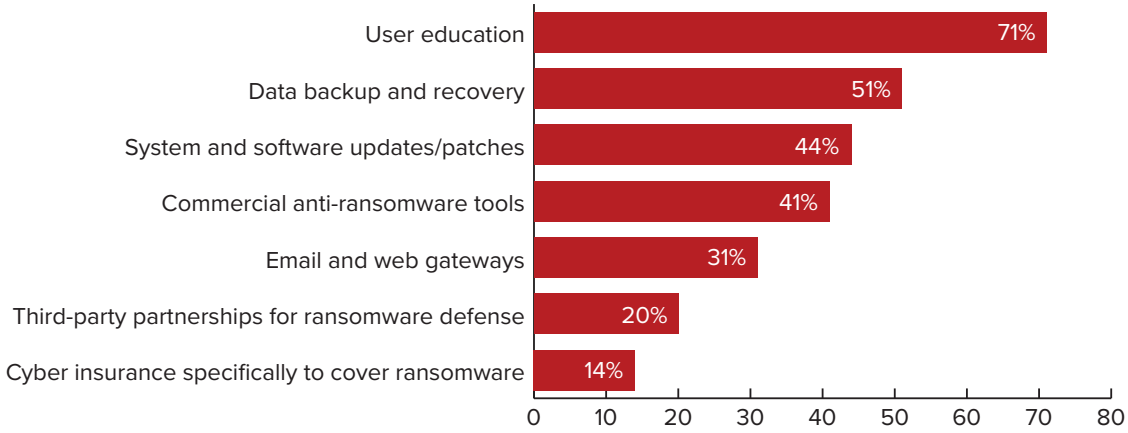
The vast majority of respondents expect equal or greater funding for ransomware defense in 2017. Where will they invest those resources? See the charts.

How do you expect your organization's budget for ransomware defense to change in 2017?



Only two percent of respondents expect a budget decrease re: ransomware defense. Nineteen percent expect an increase ranging from 1-5 percent, while 14 percent foresee a hike from 6-10 percent.

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



Top targets for ransomware defense in 2017:

- User education, which is supported by 71 percent of respondents
- Data backup and recovery – 51 percent
- System and software updates/patches – 44 percent

In the next section, the survey presentation closes with a set of conclusions drawn from the results just shared.

Then the results will be analyzed by Eduardo Cabrera of survey sponsor Trend Micro. He will offer insights to help security leaders put this survey to immediate use.

Conclusions

As the report concludes, it is useful to return to some of the original statistics that opened this report:

- 53% of respondents have been a victim of ransomware attacks in the past year.
- 60% say their biggest vulnerability is the susceptibility of their own employees.
- 65% say ransomware is most frequently encountered when users visit compromised or bogus sites.

Add to that the latest news: Researchers have now documented more than 200 different ransomware families operating in the wild. Clearly, given the growth and pace of attacks in 2016, organizations in 2017 need to take a different approach.

With that thought in mind, this report offers these four conclusions:

1. It's Time to Reassess Those Defenses

While it might be interpreted as encouraging that 59 percent of respondents believe their ransomware defenses are above average or superior, that statistic fades when held up beside the 53 percent whose organizations have been struck by ransomware attacks in the past year. With the number of ransomware families in the hundreds and with so many organizations seeing 50 or more attacks per month, traditional defenses clearly are no longer sufficient to respond–much less detect–escalating attacks. It's time for a new plan.

2. Backup Isn't a Defense

Yes, the easiest way to recover from a ransomware attack is to rely on a solid data backup and recovery plan. But that strategy still assumes your organization has been successfully attacked, and response alone is not sufficient. Organizations must put more emphasis on pure detection and defense–not just at the endpoint, but at the email and web gateways, where attacks can be both spotted and stopped.

3. User Awareness Isn't Enough

While the vast majority of respondents say their users are the weak link in the security chain and they are going to focus on improving user awareness in the coming year, where is the evidence that improving user awareness works? Remember, business email compromise has thrived alongside ransomware attacks in 2016, too, and they also rely on the user making mistakes. "Awareness" alone has not conquered that beast yet. Security leaders must continue to educate users, but they also must concede that mistakes will be made. *Then* what? That is the question to be answered with new security controls.

4. Patching Makes Perfect?

Because ransomware often compromises endpoint devices, there often is a defensive emphasis on protecting the endpoint. But that is a thankless mission, says Eduardo Cabrera, Chief Cybersecurity Officer of survey sponsor Trend Micro. There should be renewed focus on patching. "What we're seeing from the criminal underground is that many attacks utilize exploits and exploit kits and malvertisements to conduct a lot of these attacks as a vector," Cabrera says. "Attackers know organizations have challenges patching that they need to improve."

For more of Cabrera's advice, please turn to the Survey Analysis section, which follows and concludes this report.

Ransomware: The Best Defense

Survey Analysis by Eduardo Cabrera, Chief Cybersecurity Officer, Trend Micro

NOTE: In preparation of this report, ISMG VP Tom Field sat down with Eduardo Cabrera, Chief Cybersecurity Officer at Trend Micro, 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 Reax

TOM FIELD: Ed, you've seen the survey results. In what way do you find that the results validate or invalidate your own hypotheses as we went into this study?

EDUARDO CABRERA: Tom, it validates a lot of the research we're doing around ransomware attacks, as well as the data that we're receiving from our customers. We've seen a marked increase in the amount of ransomware attacks, but also have seen some differences across the different sectors. One of the bigger validation points to highlight is that the biggest impact is on business disruptions. It's quite different than your traditional type of cyberattack where intellectual property and brand reputation come into play. This type of attack is immediate and really has high consequences to organizations.

FIELD: Which of the results would you say maybe surprised you?

CABRERA: The biggest surprise we saw is that one in five of those surveyed had been attacked more than 50 times per month and that 74 percent of them were not sure that the attacks had ended. This is a huge increase in the frequency that we're seeing.

Conflicting Opinions?

FIELD: A majority of respondents say that their ransomware defenses are above average or superior, yet more than half say they also have been ransomware victims in the past year. Those seem like conflicting statements to me. What does this tell us?

CABRERA: It tells us there's probably too much trust in the traditional defenses against all attacks. And it also possibly highlights organizations' lack of understanding of the current ransomware threat. Ransomware attacks, and the criminals behind them, have been evolving for the past 10 years and have evolved even quicker with the introduction of crypto-ransomware. To put it in perspective, we've seen a five-fold increase in the amount of crypto-ransomware families we're detecting and blocking this year alone. In 2015, we tracked 29 families, and today we're tracking over 145 families since the beginning of the year. This tells us that ransomware, and the criminal enterprise behind it, is a real growth market. And cybercriminals are investing heavily in creating more capable, effective ransomware attacks. And that means network defenders must make those equal investments to protect their networks.

Eduardo Cabrera

This type of attack is immediate and really has high consequences to organizations.

Resiliency is really defined by not only speeding up detection, but it's also speeding up your patching.

Vectors and Vulnerabilities

FIELD: Ed, to get back to a point that you raised a few minutes ago, the ransomware attack frequency is higher than we might have expected at the outset of the survey. So what are your thoughts both on attack frequency and the vectors through which the attacks are coming?

CABRERA: Tom, we're definitely seeing an increase in frequency not only shown by the survey, but with the data that we have. We see spam as the primary vector of these types of attacks, but we're also seeing these criminals and these criminal groups leveraging compromised websites and malicious websites to deliver the ransomware.

FIELD: We did a lot of self-analysis in here, and we asked the respondents about their own vulnerabilities. They think that their own users are their biggest vulnerabilities. But what are your thoughts about their unpatched systems and when they lack appropriate backup for these systems?

CABRERA: I think a backup strategy is critical. We really espouse that organizations should apply the three-two-one method: They should have three different backups in two different formats and one air gapped. I think resiliency is really defined by not only speeding up detection, but it's also speeding up your patching. What we're seeing from the cybercriminal underground is that many attacks utilize exploits, exploit kits and malvertisements to conduct a lot of these attacks. Almost all exploit kits today serve up ransomware or multiple ransomware families. Attackers know organizations have these challenges patching, and they exploit this process or lack of process.

FIELD: Where do you see organizations falling down in just their basic security posture to be able to ward off ransomware attacks?

CABRERA: Unfortunately, a lot of the necessary changes ultimately are forced by organizations being breached. That usually drives the discussion and the necessary resources and improvements that are needed. Having said that, organizations need to become more proactive in their security strategy. They must take a holistic framework-first approach and make vulnerability management and protection a critical part of their overall strategy.

Evolution of Ransomware

FIELD: How specifically have you seen ransomware evolve in this past year?

CABRERA: As I mentioned earlier, we've seen 145 new families this year alone. And with each new family we're seeing changes in tactics, not only in the actual ransomware itself, but in the delivery and the ways these cybercriminals are targeting organizations. They are singling out certain departments, such as HR and payroll, and it leads to better click-through rates with much more advanced attachments such as resumes and invoices. They're improving their ability to create an environment also to scare their victims into paying the ransoms. So they're actually focusing in on the individual companies and organizations, based on the data that they're seeing.

We're also seeing an expanded customer service capability with each of these families. Some offer online chats, for example, to help victims speed up their payments and create processes for victims to pay in known currencies such as bitcoin. We're also seeing an expansion of ransomware as a service coming from the criminal underground. And cybercriminals are coming together to create enterprises to provide end-to-end ransomware services, not only in malware and ransomware development, but also execution of payment. They're able to offer services to a much wider audience. This increased level of competition in the criminal underground is creating what we see now as an escalation in frequency in paying for these types of attacks.

FIELD: The bottom line is this has turned into a pretty good business.

CABRERA: Absolutely. This has become incredibly lucrative within the criminal underground, and it's one of those burgeoning criminal enterprises that has taken over within the criminal underground.

Evolution of Response?

FIELD: In the same timeframe, how have you seen organizations response to ransomware evolve?

CABRERA: A lot of organizations now are very aware of the threat because of what we're hearing on the news and because they themselves have been targeted. Organizations still need a better understanding of the dynamic threat ransomware poses, but unfortunately they haven't gotten to the point of acknowledging the dynamic nature of this type of attack and adjusting their defenses accordingly.

Effective Elements of Defense

FIELD: Ed, throughout the survey our respondents gave us lots of insight on what they're doing to prepare and defend against ransomware. But from your experience working with organizations, what would you say are the most effective elements of preparation and defense?

CABRERA: I think the top three highlighted in the survey —user education, backup and disaster recovery, and patching—are a great start. But organizations also, as I said earlier, need to develop a framework from the top down that aligns their strategy against five basic strategic outcomes: identify, protect, detect, respond and recover from these types of attacks.

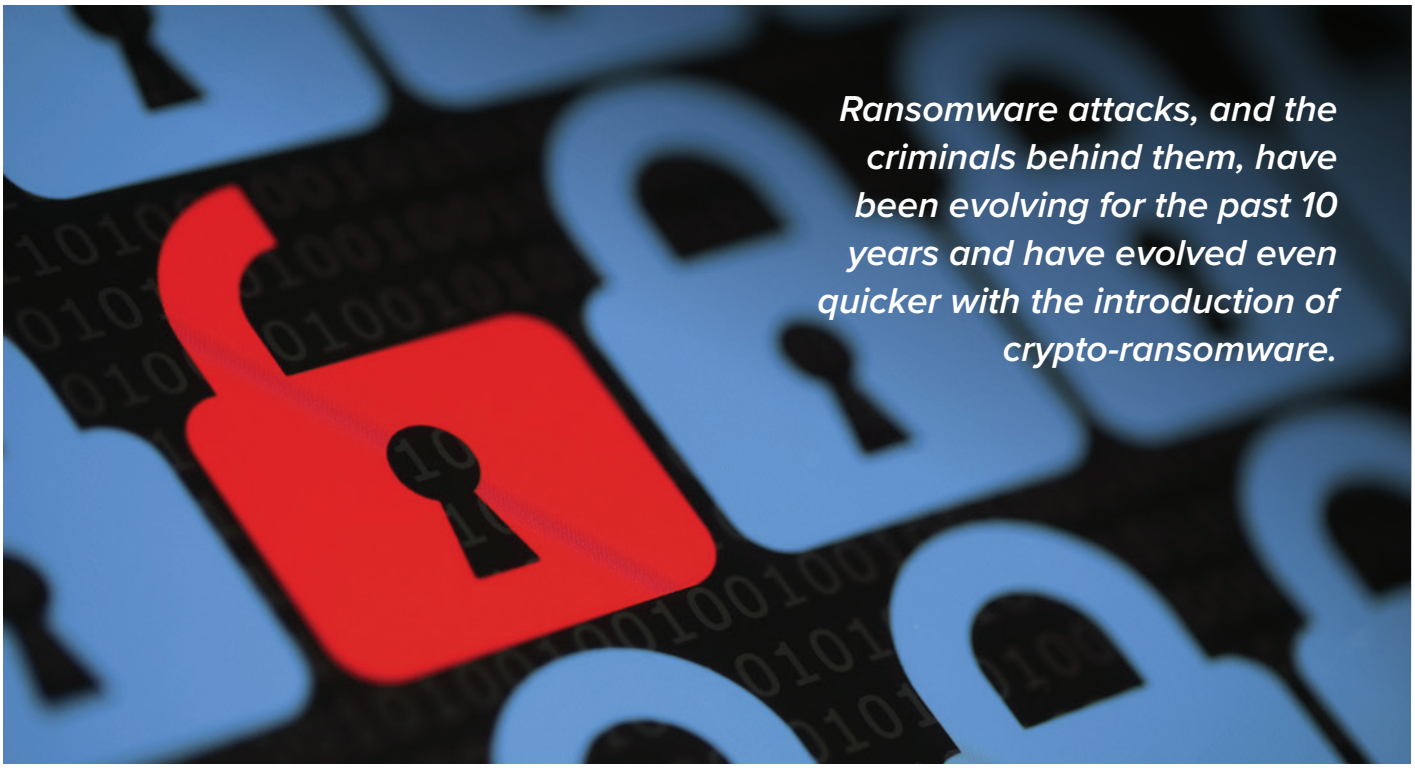
FIELD: Now how about some of the specific tools and skills? What do you think that organizations either need internally or need to get through third parties to be able to improve detection and response?

CABRERA: Tom, you really need to have the right people processes and technology in a layered, connected, threat defense strategy. It's more than just having the right tools in your security stack. You also need to be able to communicate and collaborate with one another. The right people and processes make a difference to effectively create a strategic outcome that you want, and that's a more resilient and secure network for your users.

2017 Investments

FIELD: Based on what you've learned this year, where do you recommend that organizations invest their ransomware defense resources in 2017?

CABRERA: Each organization is different. They really need to establish a robust risk-management strategy that really starts with understanding what is the most vulnerable data that they have, as well as the infrastructure holding that data, so they can build proper security solutions around it. With ransomware specifically, having a gateway protection for email and web is critical, as well as having a robust endpoint solution. Machine learning capabilities at the end point are critical going forward to make these types of investments pay off. Our security must be one step ahead of the ransomware as the latter continues to evolve.



Ransomware: What's Next?

FIELD: What ransomware trends might we expect to see in the next year?

CABRERA: Like all cyberattacks, ransomware will continue to evolve. Individuals behind these attacks are evolving and their tactics as well. So what we'll see going forward is a move from static data being encrypted to live, dynamic data being impacted, such as streaming services or any service that provides real-time data for their customers or their other business partners. Cybercriminals are going to pivot and apply the model they've created with traditional ransomware and migrate it to use against other platforms. Therefore, we need to think outside the box and try to understand what is critical to each of our organizations if impacted by some sort of ransomware attack.

Pay the Ransom?

FIELD: Now I have to ask you the same question we asked our respondents up front: Should we ever pay the ransom?

CABRERA: Tom, my answer is no. At the same time, I completely understand that a lot of organizations find themselves ill prepared and have to—or feel they have to—pay to get their data back. Because if you go down the road of paying these cybercriminals, it does not necessarily mean that you're going to get your data back intact. There's a huge question of integrity of that data if and when you get it back. We're also seeing cybercriminal crews within the underground that are not releasing the data even after being paid.

FIELD: And bottom line, if organizations stop paying the ransom, this would stop being a lucrative crime.

CABRERA: Absolutely. And the other issue here is that you create a market. You've essentially told the world that you're willing to pay ransoms, and you're increasing the likelihood of additional attacks going forward.

Put Survey to Work

FIELD: Ed, we've covered a lot of topics in our discussion here from defenses, to response, to the trends that you're seeing and the ransomware variants. It's an overwhelming amount of information. How do you recommend that our audience put these survey results to use in their own organizations to improve their defenses?

CABRERA: I think they really need to take the survey and look at how they are positioned and look at ways to improve their security. They need to look at this threat, like any other threat, and really evaluate the threats that they're facing, but also the vulnerabilities that they have and how could they be better positioned and more resilient against these types of attacks. ■

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 Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY® Prevention. Response. Notification.

ISMG INFORMATION SECURITY MEDIA GROUP

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