SURVEY REPORT

Second Annual State of Ransomware Report: Survey Results for France

An Osterman Research Survey Report

Published July 2017

Sponsored by

Malwarebytes

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

TABLE OF CONTENTS

FRANCE

EXECUTIVE SUMMARY

This survey report presents the results of a survey undertaken in France as part of a larger survey of organizations in five additional geographies – the United States, United Kingdom, Germany, Australia and Singapore – on ransomware and other critical security issues. The survey was conducted with small- to mid-sized businesses during June 2017 with 175 organizations in France and 175 to 179 in each of the other five nations. In order to qualify for participation in the survey, respondents had to be a) responsible and/or knowledgeable about cybersecurity issues within their organization, and b) the organizations surveyed could have no more than 1,000 employees. A total of 22 questions were in included in the survey. Results from the other surveys are available in separate national and regional survey reports.

THE AFTERMATH OF RANSOMWARE

- **The impact of ransomware on small to mid-sized businesses can be very damaging**
  Among small to mid-sized French organizations that have experienced a successful infiltration of the corporate network by ransomware, a staggering 34 percent reported that they had to cease business operations immediately (dramatically higher than the global average of 20 percent), and 16 percent lost revenue (slightly higher than the global average).

- **Ransom demands are second to downtime as the biggest problem with ransomware**
  We found that for about one-half of the French organizations that were infected with ransomware, the ransom demanded was $1,000 or less. In fact, only 16 percent of ransom demands were in excess of $10,000 and only two percent were for more than $50,000. However, our research also found that for eight percent of impacted organizations, a ransomware infection caused 25 or more hours of downtime. French organizations generally suffered less ransomware-induced downtime than their counterparts globally, but downtime was still significant.

- **For many organizations, the source of ransomware is unknown**
  The most common source of ransomware infections in French organizations is not known: 41 percent reported that the source of their most severe ransomware infection could not be identified, which was significantly higher than the global average of 27 percent.

- **Ransomware infections often spread once they take hold**
  Our research found that in many ransomware attacks the infection is not limited to a single endpoint, but can spread to others, as well. However, unlike what we found in other countries, the infection did not spread to every endpoint on the network in the French organizations we surveyed. Organizations in France were a bit less likely than the global average to see ransomware infections spread to more than just the initial endpoint that was infected.

ATTITUDES ABOUT PAYING RANSOMWARE

- **Most small to mid-sized businesses do not believe in paying ransomware demands**
  We found that a sizeable majority of French respondents believe that ransomware demands should never be paid (67 percent in France versus the global average of 59 percent), while the remaining organizations believe they should be paid if the encrypted data is of value.

- **For those that did not pay the ransom, many lost files as a result**
  We found that among the French organizations we surveyed that did not pay the ransom that was demanded of them, 25 percent lost files, significantly lower than the global average of 25 percent.

- **Most organizations consider addressing ransomware to be a high priority, but they don't have much confidence in their ability to deal with it**
  The vast majority of organizations give a high or very high priority to addressing the ransomware problem (88 percent of the French organizations surveyed versus 75 percent globally); to investing in resources, technology and funding to address the problem (82 percent compared to 67 percent globally); but much less to investing in education and training about ransomware for end users (44 percent versus 53 percent globally).

  Despite these investments, fewer than one-third of the French organizations surveyed expressed little to only moderate confidence in their ability to stop a ransomware attack. In fact, only 14

percent of organizations surveyed felt "very confident" in their ability to thwart ransomware attacks, but this was higher the global average of 10 percent.

RANSOMWARE TECHNOLOGY TRENDS

- **Small to mid-sized businesses believe fighting ransomware is more about training user than implementing technology**
  When asked if ransomware should be addressed only through technology or only through training, many more French organizations believe the latter will be more effective in addressing the ransomware problem, which is contrast to the global view that technology is more effective. Although the remaining 88 percent of survey respondents believe that a mix of technology and training are necessary, French organizations tilt decidedly more toward training-based approaches as more effective.

- **However, current technology usage does not seem to be sufficient to address the problem adequately**
  Our research found that French organizations have implemented a variety of solutions to address their ransomware concerns, either before or after the fact. French organizations are much more likely to implement on-premises backups, email security and on-premises ransomware solutions than their global counterparts; but less likely to deploy cloud-based backup and cloud-based ransomware solutions.

ABOUT THIS SURVEY AUDIENCE

The distribution of industries surveyed in France is shown in Figure 1. These organizations had a mean of 385 employees and 200 email users.

Figure 1
Distribution of Organizations Surveyed

Industry	%
Engineering/Construction	25%
Manufacturing	16%
Transportation	10%
Food/Agriculture	8%
Retail/E-commerce	7%
Education	4%
Hospitality	4%
Financial services/Banking/Insurance	3%
High tech	3%
Government	2%
Healthcare	1%
Pharmaceutical	1%
Law enforcement	0%
Other	15%

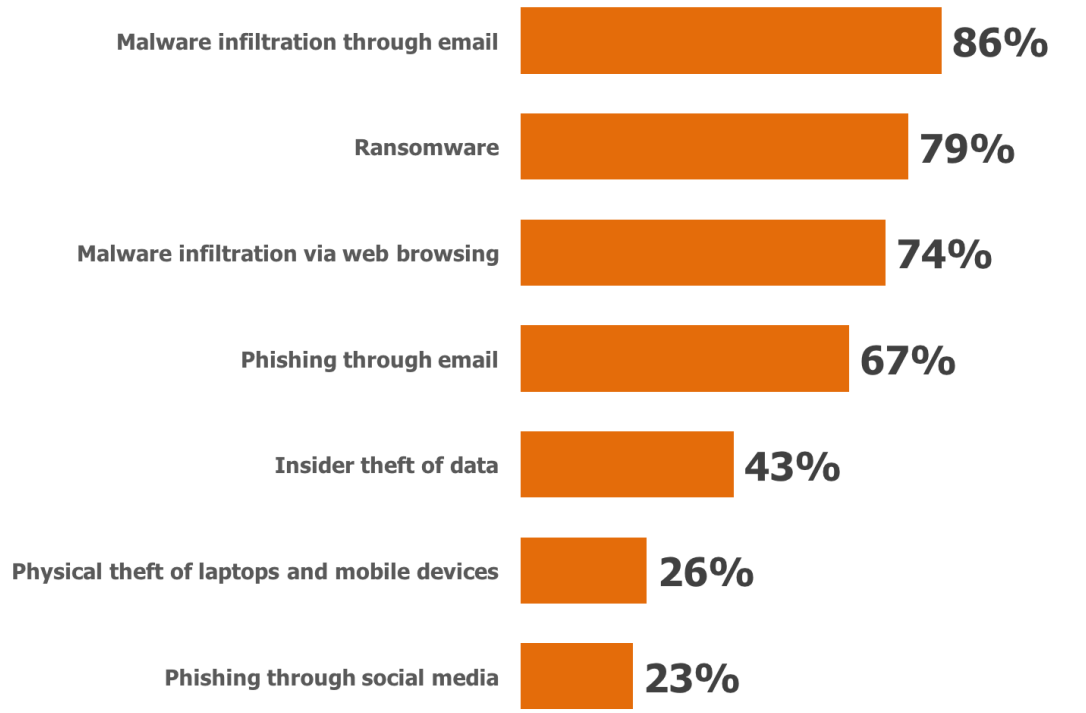
Source: Osterman Research, Inc.

RANSOMWARE IS A CRITICAL PROBLEM

RANSOMWARE IN THE CONTEXT OF OTHER SECURITY THREATS

Ransomware is an increasingly serious issue, and the problem is getting worse over time. As shown in Figure 2, ransomware is the second most serious problem for organizations in France, cited by 79 percent of those surveyed as a problem about which they are "concerned" or "extremely concerned" (significantly higher than the global average of 69 percent). Our research found that the average level of concern about the issues shown in Figure 2 (those indicating that they are "concerned" or "extremely concerned") was within a fairly tight band across all of the geographies we surveyed, ranging from a low of 51.9 percent in Germany to a high of 58.5 percent in the United States. However, the range for the concern over ransomware varied more significantly, from a low of 57.7 percent in Australia to a high of 78.9 percent in France.

Figure 2
Concern About Various Security Threats
Percentage Responding Concerned or Extremely Concerned



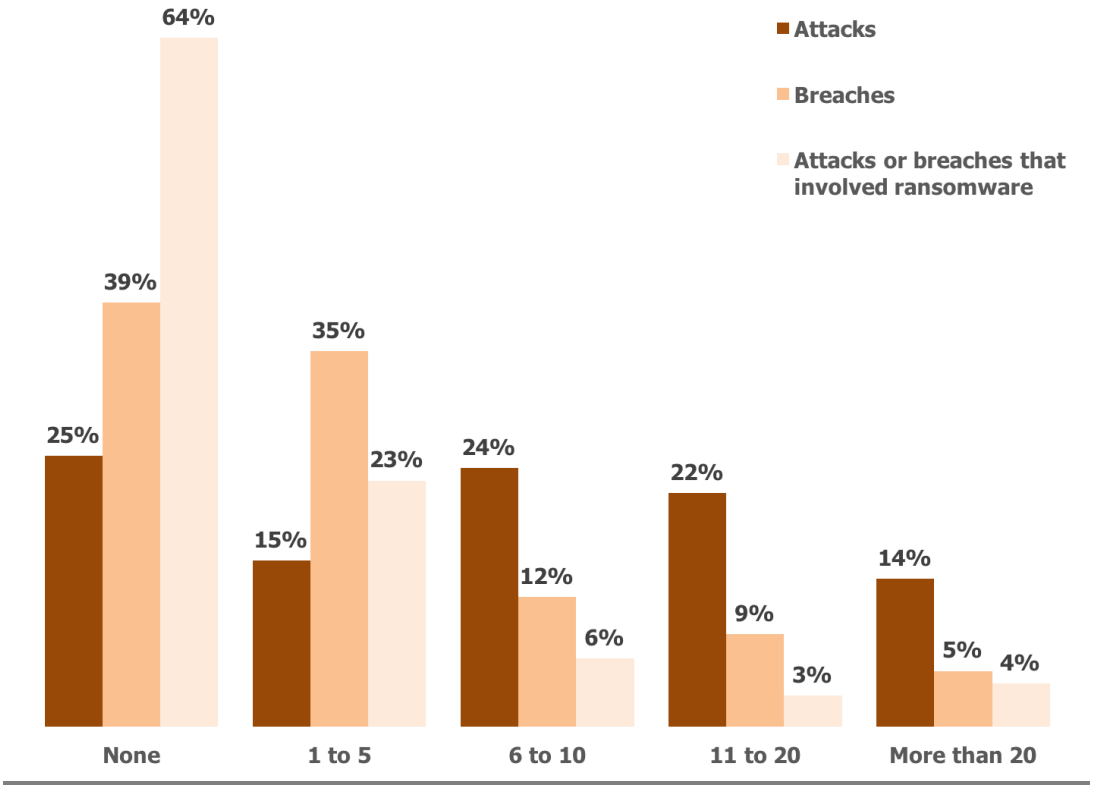
Source: Osterman Research, Inc.

F R A N C E

HOW COMMON ARE RANSOMWARE AND OTHER THREATS?

As shown in Figure 3, most organizations in France have experienced various types of security attacks and data breaches over the past year, with many organizations experiencing some type of security-related incident on a more than monthly basis. Also of note is that 36 percent of French organizations have experienced a ransomware attack during the last 12 months, with most of those having been victimized seeing anywhere from one to five such attacks during the past year. The French companies we surveyed actually rank a bit better globally with regard to attacks and breaches, but slightly worse in the context of ransomware.

Figure 3
Attacks, Breaches and Ransomware Infiltrations During the Previous 12 Months



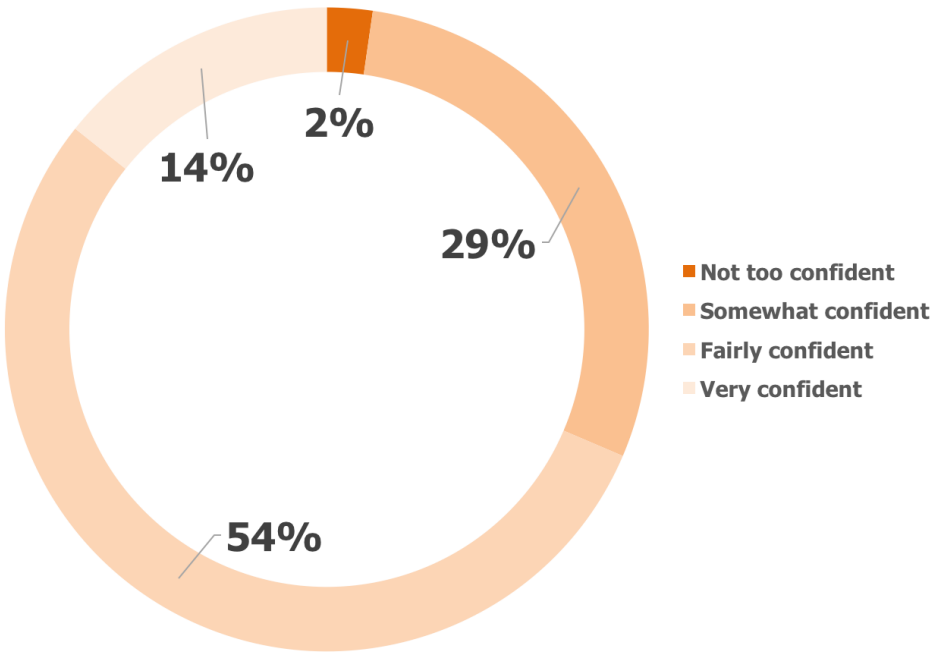
Source: Osterman Research, Inc.

F R A N C E

CONFIDENCE IN ADDRESSING THE RANSOMWARE PROBLEM

French organizations' confidence among decision-makers about their ability to stop a ransomware attack is not very high. As shown in Figure 4, 31 percent of organizations has relatively little confidence that they can stop a ransomware attack that has infiltrated their network. However, 68 percent of French organizations are "fairly" or "very" confident that it can thwart a ransomware attack, significantly higher than the global average of 54 percent.

Figure 4
Level of Confidence That a Ransomware Attack Can be Stopped



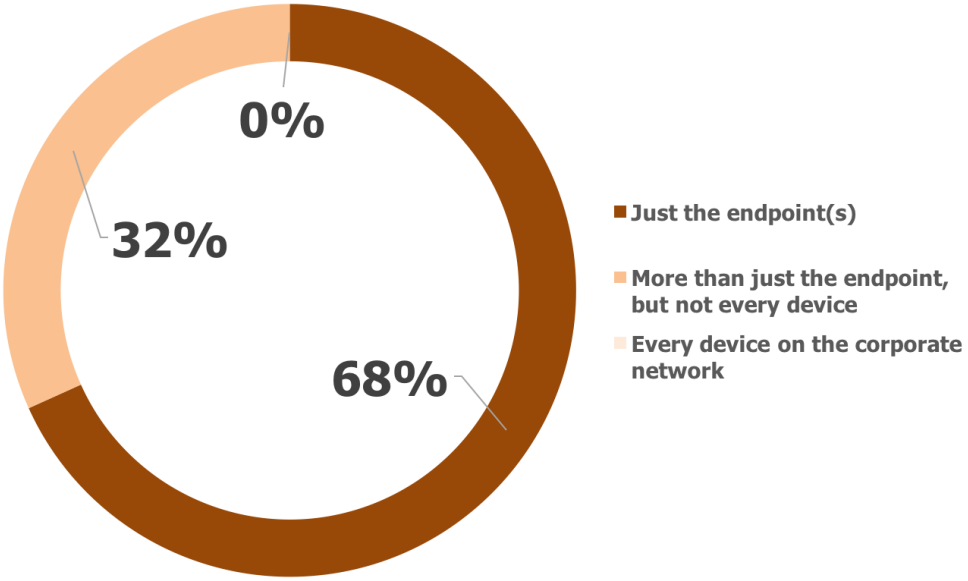
Source: Osterman Research, Inc.

HOW ORGANIZATIONS RESPOND TO RANSOMWARE AND HOW THEY'RE IMPACTED

THE IMPACTS OF RANSOMWARE CAN BE DEVASTATING

The impact of ransomware can be damaging to an organization. As shown in Figure 5, our research found that while most of the ransomware incidents that have been experienced involved just the endpoint, 32 percent of these infections spread to other devices, although for none of the French organizations we surveyed had the ransomware infection impacted every device on the network. The spread of ransomware was actually a bit better among French companies than across all of the six geographies we surveyed, with "only" 32 percent of French organizations seeing a spread beyond the initial endpoint versus 37 percent globally.

Figure 5
Extent of the Most Serious Ransomware Attack That Has Been Experienced



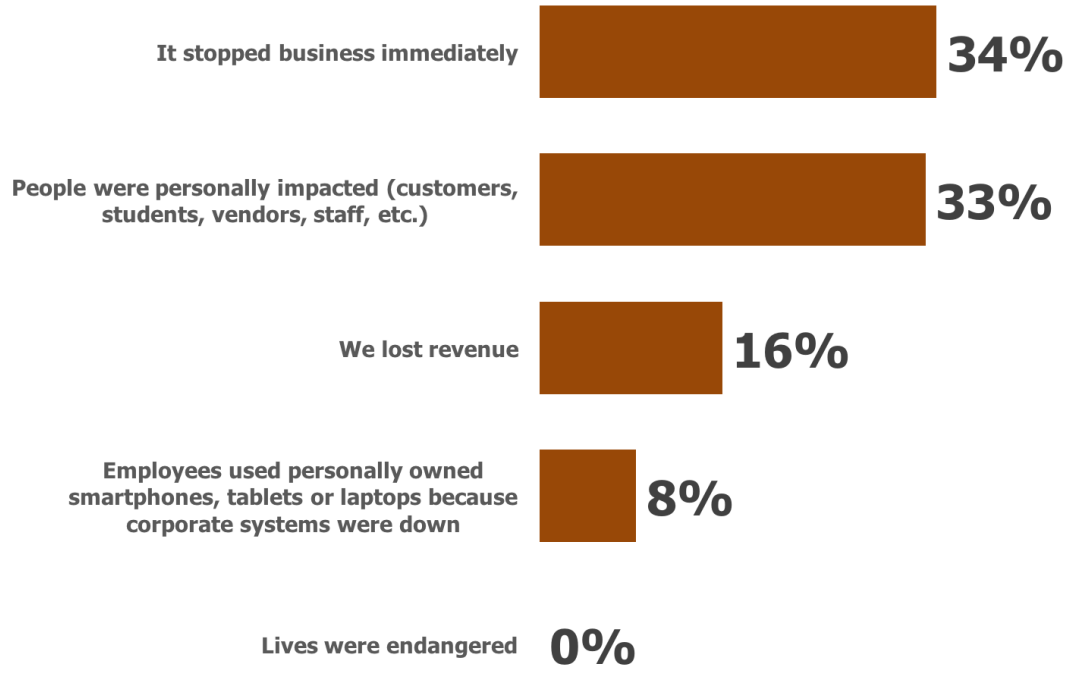
Source: Osterman Research, Inc.

The survey found some level of variability in the proportion of endpoints that were infected by the most serious ransomware infection that had impacted organizations. For example, organizations in Germany and the United States experienced the greatest proportion of network/every endpoint-wide infections at 5.0 percent and 4.3 percent, while no organizations surveyed in France or Singapore reported ransomware infections that impacted every device on the network. By contrast, 68.3 percent of French organizations reported that only a single endpoint was infected by the most severe ransomware infection they had experienced, as shown above, whereas this figure was "only" 50.7 percent for Australian organizations.

FRANCE

Infections from ransomware attacks create a wide range of consequences. As shown in Figure 6, the most serious impact for 34 percent of French organizations was that it stopped business immediately, significantly worse than the global average of 22 percent. Other impacts from ransomware included employees using personally owned devices like smartphones and tablets instead of corporate systems and lost revenue (about on par with the global average).

Figure 6
Impact of the Most Serious Ransomware Attack That Has Been Experienced

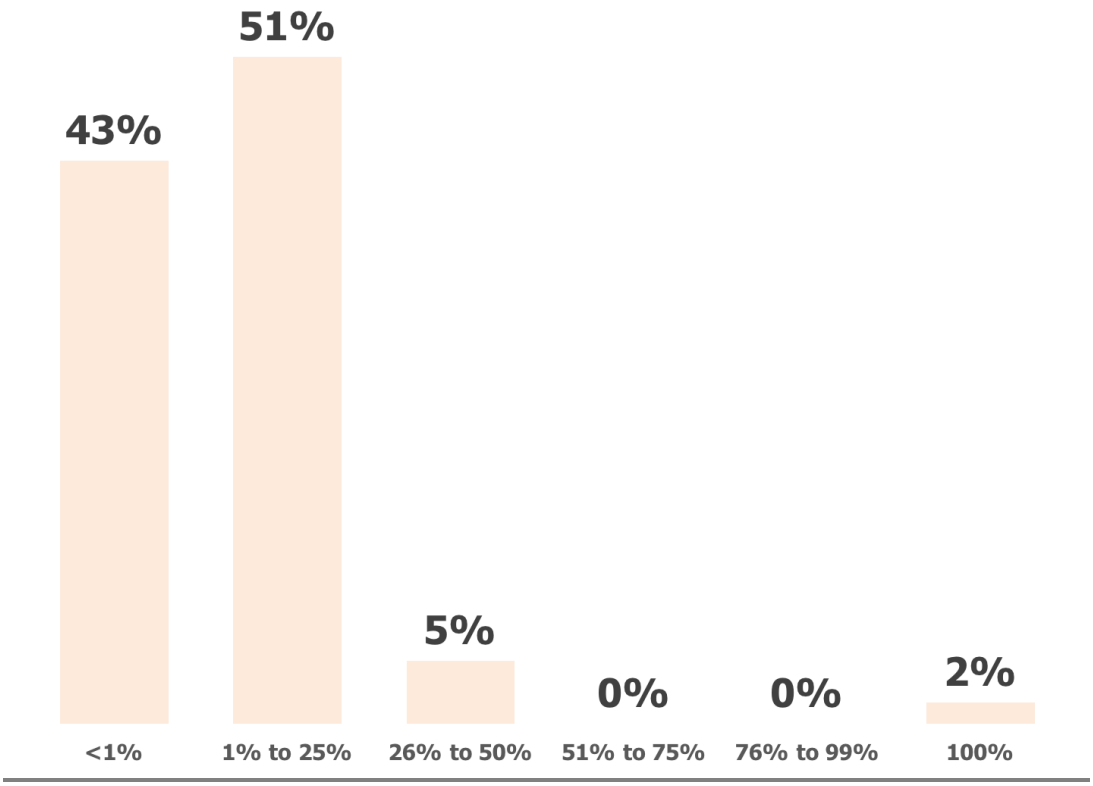


Source: Osterman Research, Inc.

FRANCE

As shown in Figure 7, 43 percent of the organizations in France that fell victim to ransomware had fewer than one percent of their endpoints infected, while another one-half had up to 25 percent infected. However, the remaining organizations had more than 25 percent of their endpoints infected. However, the situation in France is actually much better than it is globally: only seven percent of French organizations experienced more than 25 percent of their endpoints infected with ransomware from the most severe infection they experienced versus 26 percent of organizations globally.

Figure 7
Proportion of Endpoints Infected in the Most Serious Ransomware Attack That Has Been Experienced



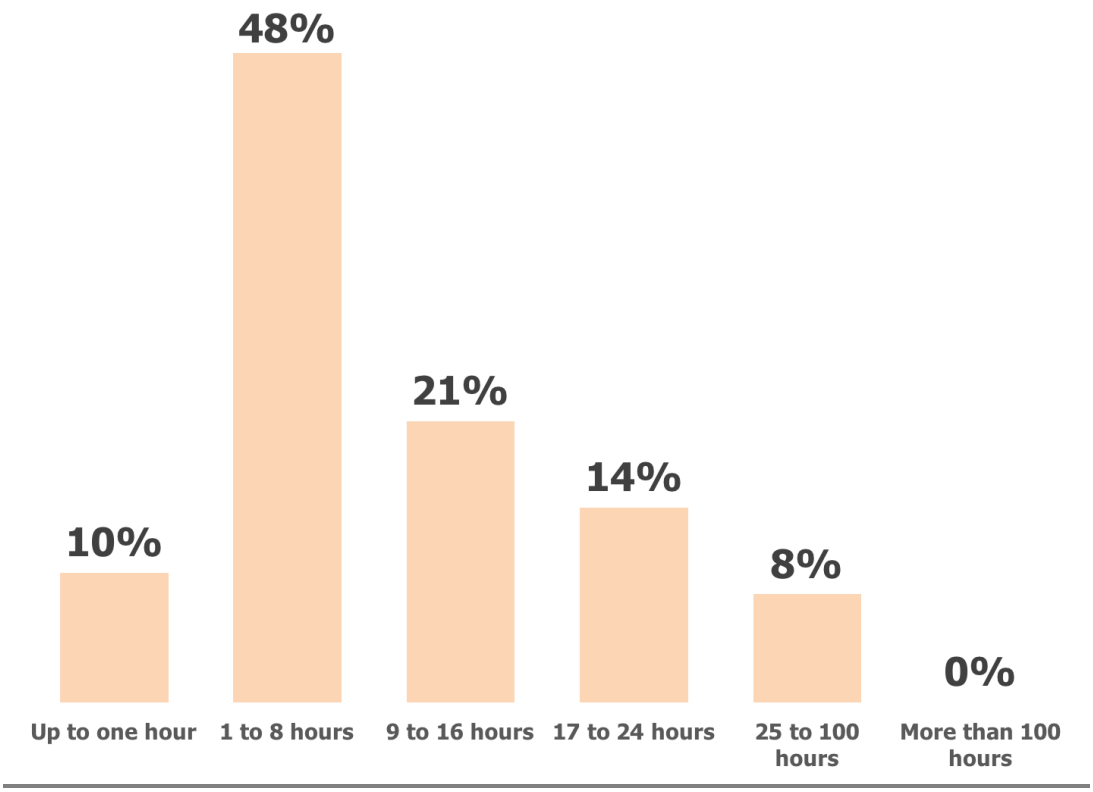
Source: Osterman Research, Inc.

FRANCE

Ransomware-induced downtime is a major consequence for many ransomware infections because an infected endpoint becomes immediately unavailable. A rapid restoration of an infected endpoint can minimize downtime, but as shown in Figure 8, fast recovery from ransomware is not common, with most experiencing anywhere from one day to almost two weeks of downtime from a ransomware attack.

Our research found that only 10 percent of organizations had minimal downtime (no more than one hour) resulting from ransomware, but almost one-half of organizations experienced anywhere from one to eight hours of downtime. However, it gets worse: 43 percent of organizations infected by ransomware experienced nine or more hours of downtime.

Figure 8
Downtime Experienced in the Most Serious Ransomware Attack That Has Been Experienced



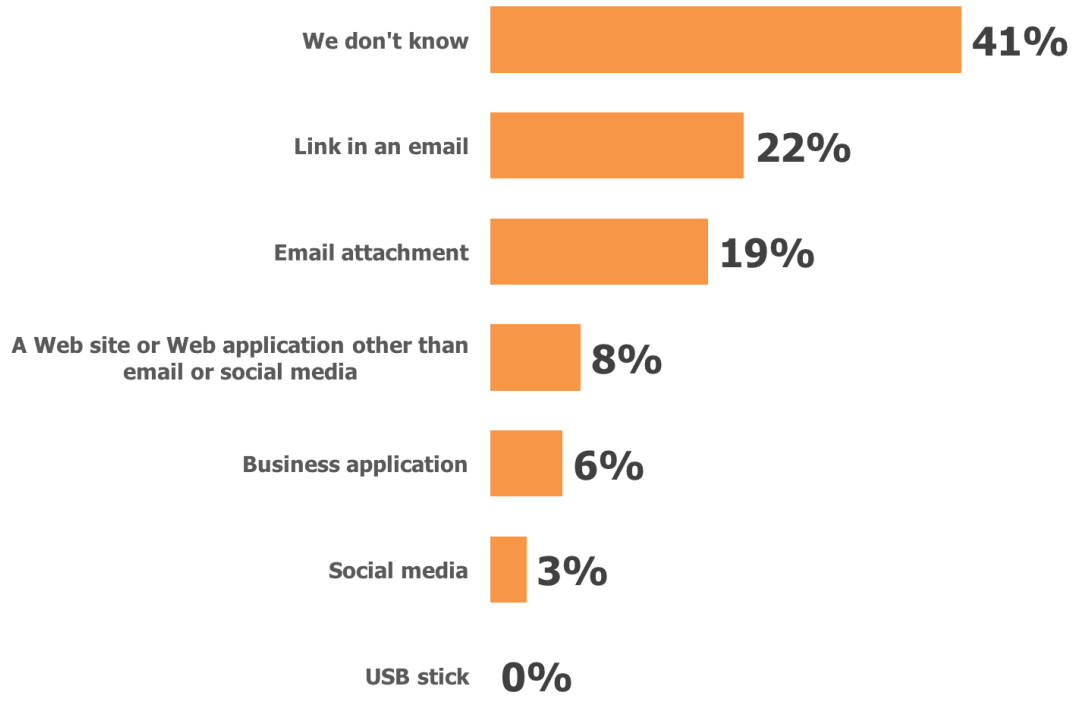
Source: Osterman Research, Inc.

FRANCE

HOW DOES RANSOMWARE ENTER AN ORGANIZATION?

The most commonly cited source of a ransomware infection in French organizations was not known: 41 percent organizations reported that they did not know the source of their most severe ransomware infection, as shown in Figure 9. This was significantly higher than the global average of 27 percent. Where sources of the infection were known, 22 percent reported it came from a malicious link in an email and 19 percent from an email attachment, both lower than the global averages of 23 percent and 24 percent, respectively.

Figure 9
Manner by Which Malware Entered in the Most Serious Ransomware Attack That Has Been Experienced



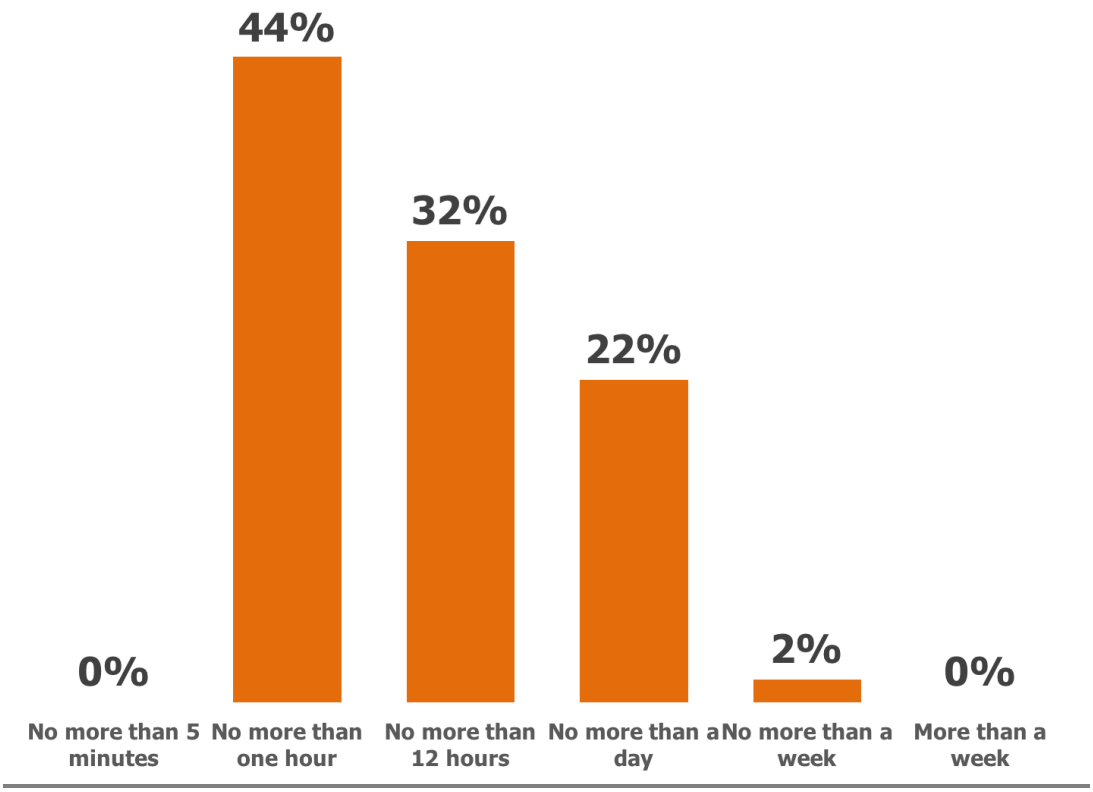
Source: Osterman Research, Inc.

F R A N C E

HOW DOES IT RESPOND TO RANSOMWARE?

The length of time that elapses between the initial ransomware infection and its detection is critical to stopping the spread of the infection. As shown in Figure 10, none of the French organizations we surveyed could detect a ransomware infection in five minutes or less. Another 44 percent could do so more in no more than one hour after an endpoint was infected, but more than one-half of the organizations surveyed in France required many hours or even days before they detected the problem. The results we discovered among organizations in France were worse than the overall global results.

Figure 10
Time Elapsed Before Detection in the Most Serious Ransomware Attack That Has Been Experienced



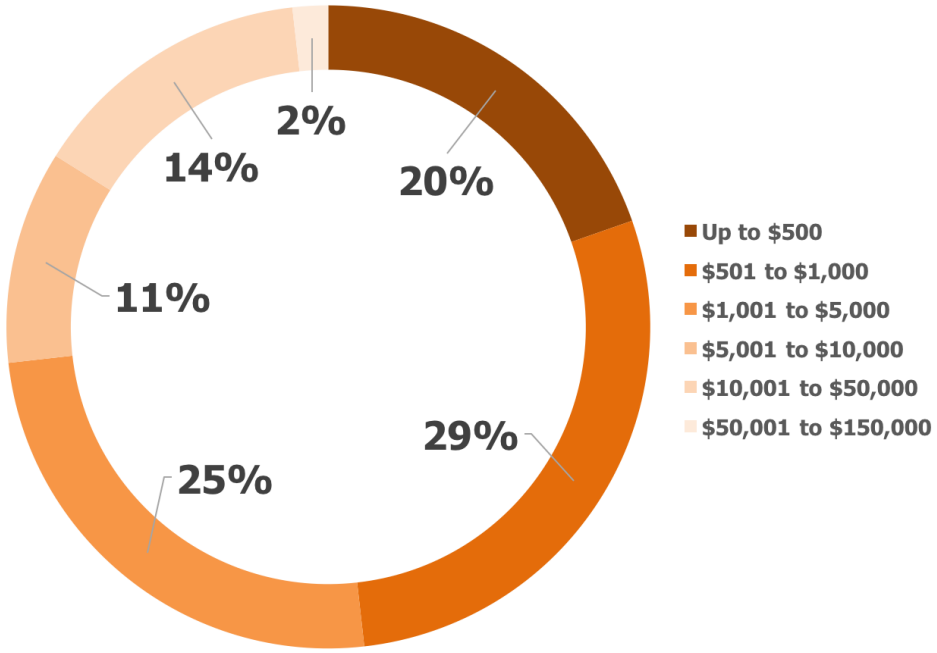
Source: Osterman Research, Inc.

F R A N C E

AMOUNTS THAT CYBER CRIMINALS HAVE DEMANDED AND RESPONSES TO THESE DEMANDS

Most ransom demands from cyber criminals are fairly small: as shown in Figure 11, about one-half of these demands of small to mid-sized businesses ask for less than $1,000. However, many cyber criminals ask for much larger sums, with 51 percent asking for more than $1,000 and two percent demanding up to $150,000. The results we found for organizations in France were somewhat different than those we discovered in the other geographies: while 49 percent of French organizations were hit with ransom demands of up to $1,000, 55 percent of firms globally experienced this level of "inexpensive" extortion.

Figure 11
Amount Demanded in the Most Serious Ransomware Attack That Has Been Experienced

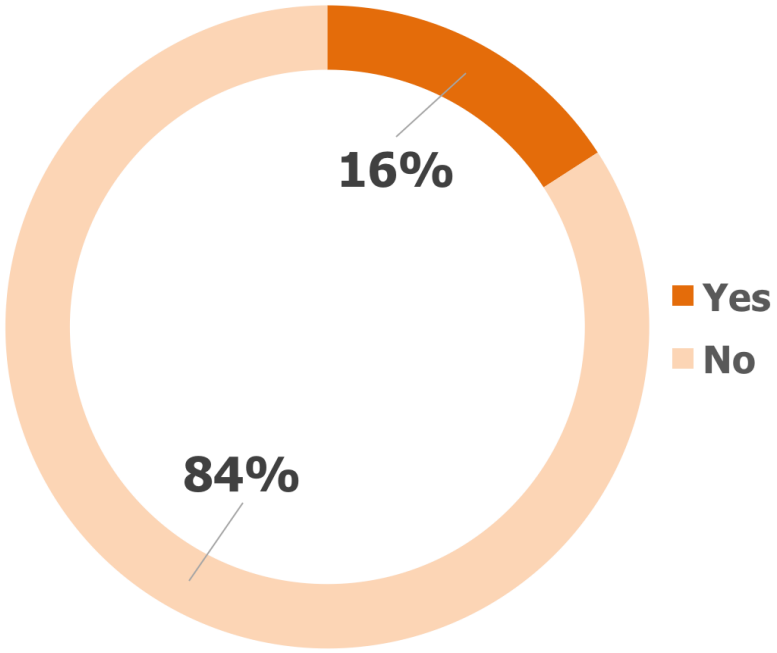


Source: Osterman Research, Inc.

FRANCE

Among French organizations that were infected with ransomware, only about one in six opted to pay the ransomware demands, as shown in Figure 12 (this was substantially lower than the global average of 28 percent). However, we found significant variability between the geographies that we surveyed. For example, in addition to France's low likelihood of payment and 17 percent of German organizations opting to pay the ransom demanded after their most severe ransomware infection, 43 percent of British and 46 percent of Australian organizations opted to do so.

Figure 12
Was Ransom Paid in the Most Serious Ransomware Attack That Has Been Experienced?

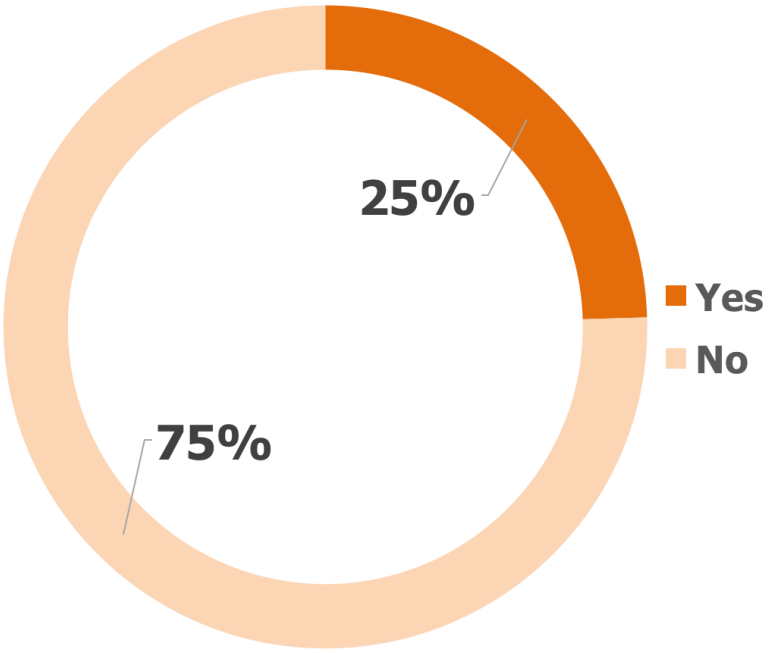


Source: Osterman Research, Inc.

FRANCE

Among French organizations that chose not to pay cyber criminals' ransom demands, one quarter lost files as a result of their decision not to pay, as shown in Figure 13. Here, too, we found significant variability among the organizations based on geography. For example, British and Australian organizations experienced the greatest degree of file loss from their decision not to pay – 46 percent and 40 percent, respectively. Organizations in Germany and France were the least likely to lose files from their decision not to pay ransom demands. Globally, 32 percent of organizations that opted not to pay ransom demands lost files, resulting in French firms being significantly lower than the average for file loss.

Figure 13
Were Files Lost in the Most Serious Ransomware Attack That Has Been Experienced Among Organizations That Did Not Pay the Ransom?



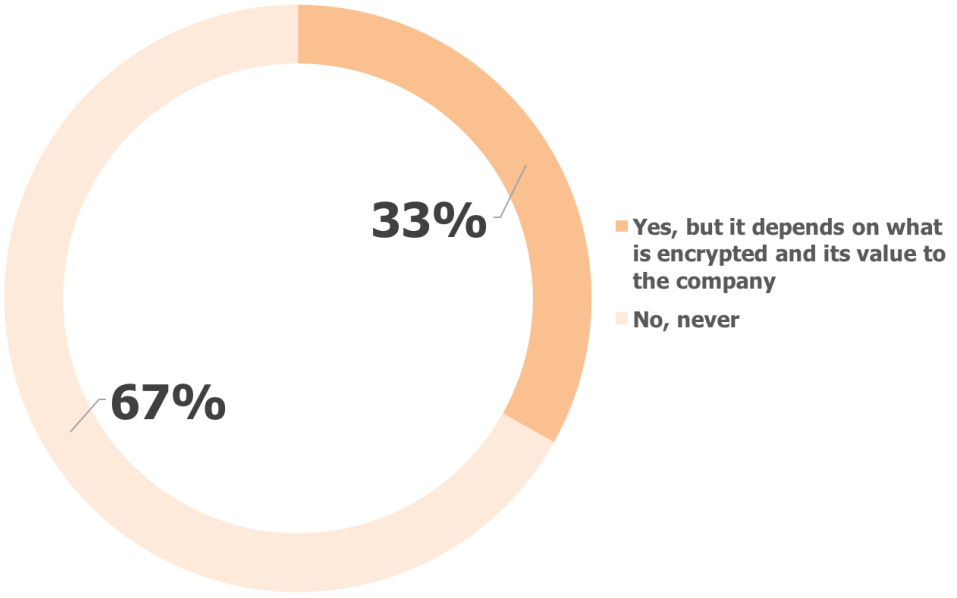
Source: Osterman Research, Inc.

F R A N C E

SHOULD ORGANIZATIONS PAY RANSOMWARE DEMANDS?

When infected by ransomware, decision makers face a difficult decision: should they pay the ransomware to recover their files and potentially increase their chances of being infected again by demonstrating a willingness to pay, or should they refuse to pay and suffer the consequences? As shown in Figure 14, most organizations in France believe, at least in general, that organizations should not pay ransomware demands. Organizations in France are less likely to believe that companies should pay ransom demands: 33 percent versus the global average of 41 percent.

Figure 14
Belief That Companies Should Pay Ransom Demands if They Are Hit With Ransomware

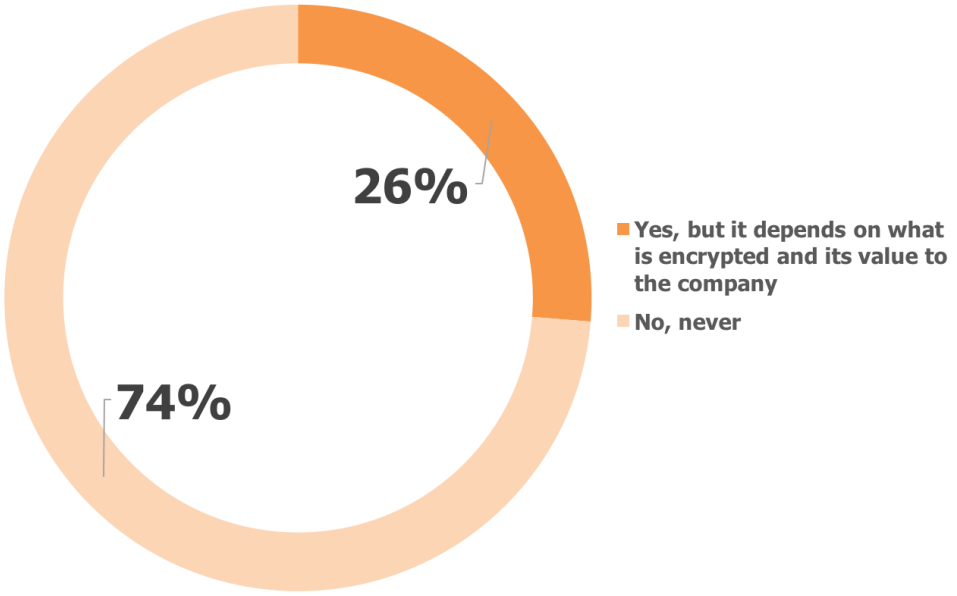


Source: Osterman Research, Inc.

FRANCE

We also asked survey respondents to personalize the decision of whether or not to pay ransom demands. As shown in Figure 15, the results about the decision to pay a ransom whether or not respondents were answering about organizations in general or their own organization were quite different: whereas when asked about organizations in general, French respondents indicated that 33 percent should pay, but this figure dropped to 26 percent when it came to their own organization. That said, French organizations are much less open to the idea of paying ransom than are their global counterparts.

Figure 15
Do You Believe That Your Company Should Pay Ransom Demands If You Are Hit With Ransomware?



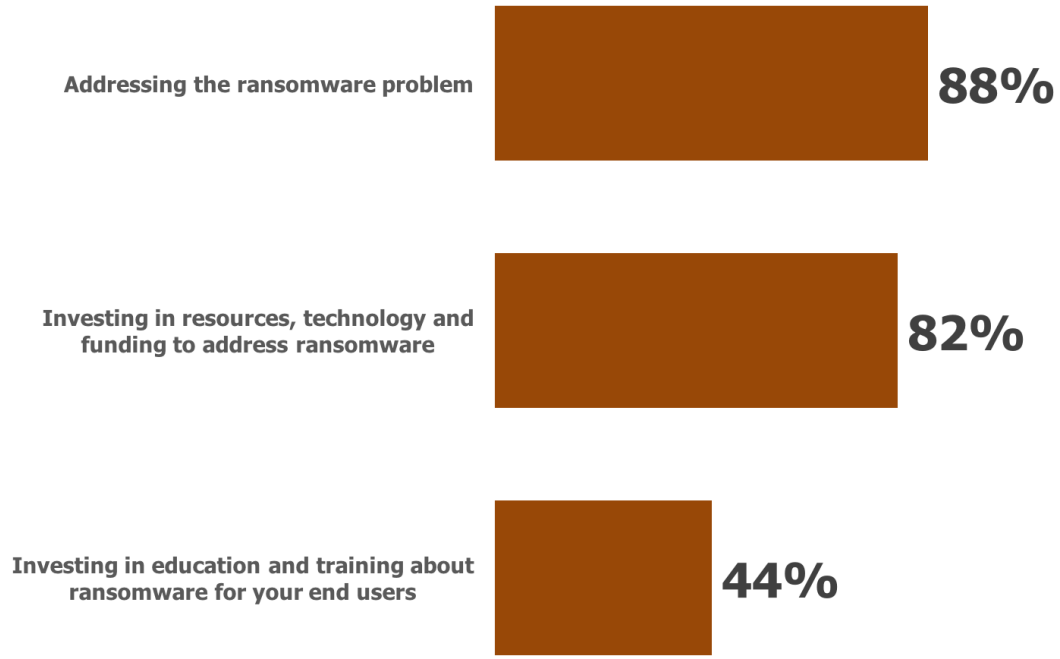
Source: Osterman Research, Inc.

THE IMPORTANCE OF ADDRESSING THE RANSOMWARE PROBLEM

THE NEED TO SOLVE THE RANSOMWARE PROBLEM

Decision makers are strongly in agreement that the ransomware problem needs to be solved and they are addressing it as a high priority. As shown in Figure 16, 88 percent of French survey respondents give a "high" or "very high" priority to addressing the ransomware problem (much higher than the global average of 75 percent); 82 percent give investing in resources, technology and funding to address ransomware this high a priority (also much higher than the global average of 67 percent); but only 44 percent consider that investing in user education and training about ransomware needs to be a high or very high priority (versus 53 percent globally).

Figure 16
Priorities for Addressing Various Aspects of the Ransomware Problem
Percentage Responding a High or Very High Priority



Source: Osterman Research, Inc.

F R A N C E

IS SOLVING RANSOMWARE A HUMAN OR TECHNOLOGY ISSUE?

The debate about how best to solve the ransomware problem is an ongoing issue: should the primary or only focus be on user training, or should the focus be primarily exclusively on a technology-oriented approach? As shown in Figure 17, only one percent of the French organizations surveyed believe that ransomware can be addressed properly only through a technology-focused approached, while another 10 percent believe that the problem is best addressed mostly using anti-ransomware technology. By contrast, 60 percent of respondents believe that the primary focus of anti-ransomware approaches should be directed toward training users.

Figure 17
Extent to Which Organizations Believe That Solving the Ransomware Problem is a Human vs. Technology Issue

Source: Osterman Research, Inc.

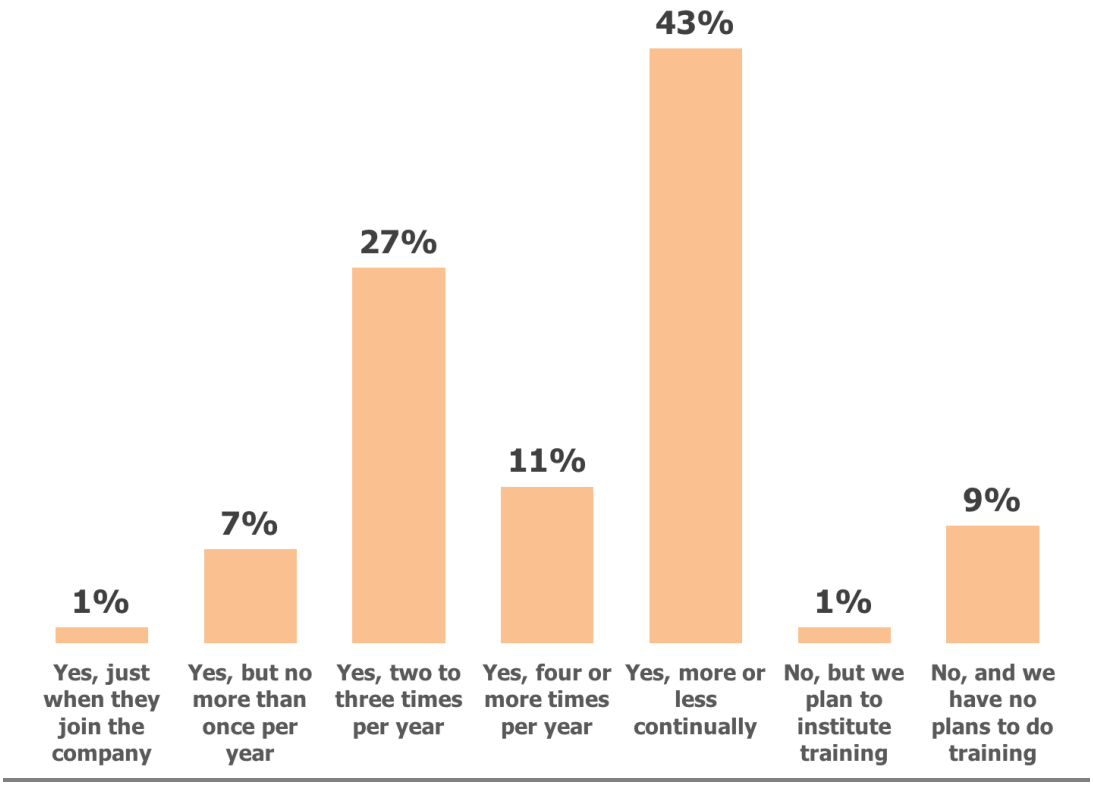
Organizations in France are significantly more focused on security awareness training than organizations globally. For example, while 39 percent of organizations globally believe that addressing ransomware is primarily a technology-focused issue versus only 11 percent in France. The opposite is true with regard to security awareness training: 60 percent of French organizations believe in a primarily training-based approach to deal with ransomware versus 30 percent globally.

FRANCE

THE ROLE OF SECURITY AWARENESS TRAINING

As shown in Figure 18, ten percent of organizations in France do not conduct security awareness training that specifically addresses ransomware. Among the 90 percent of French organizations that conduct some form of training, 43 percent do so more or less continually, which is more than 2.5 times higher than the global average of 16 percent. Overall, French organizations are much more proactive with regard to ransomware-related security awareness training: 81 percent of French organizations conduct this training at least twice per year versus only 47 percent of organizations globally.

Figure 18
Do Employees Go Through Security Awareness Training that Specifically Mentions Ransomware and Frequency of This Training



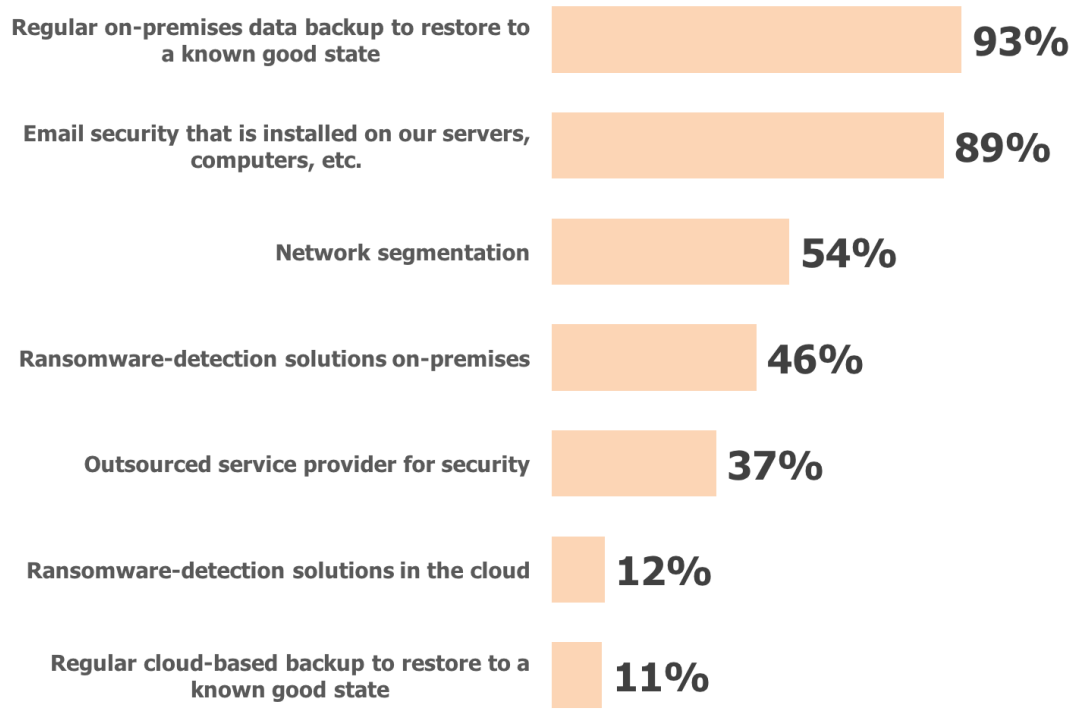
Source: Osterman Research, Inc.

F R A N C E

TECHNOLOGIES/PROCESSES IN PLACE TO ADDRESS RANSOMWARE

The vast majority of the French organizations we surveyed have deployed both regular, on-premises backup solutions and processes, as well as email security, to address the ransomware problem, as shown in Figure 19. Many organizations also have implemented network segmentation, the use of outsourced security providers, ransomware-detection solutions, and regular, cloud-based backup capabilities. We found that French firms are much more likely to have deployed on-premises backups to deal with ransomware than their global counterparts (93 percent in France versus 69 globally), as well as email security solutions (89 percent in France versus 82 percent globally). While French organizations have a higher penetration of on-premises ransomware solutions (46 percent versus 37 percent globally), they have a lower penetration of cloud-based ransomware solutions (12 percent in France versus 21 percent globally).

Figure 19
Technologies and Processes in Place to Address Ransomware



Source: Osterman Research, Inc.

ABOUT MALWAREBYTES

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts. For more information, please visit us at http://www.malwarebytes.com/.

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. Marcin was recently named "CEO of the Year" in the Global Excellence awards and has been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and the Silicon Valley Business Journal's 40 Under 40 award, adding those to an Ernst & Young Entrepreneur of the Year Award.