SURVEY REPORT

Second Annual State of Ransomware Report: Survey Results for Germany

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

GERMANY

TABLE OF CONTENTS

GERMANY

EXECUTIVE SUMMARY

This survey report presents the results of a survey undertaken in Germany as part of a larger survey of organizations in five additional geographies – the United States, United Kingdom, France, 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 Germany 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

- **Ransomware in small to mid-sized businesses can be very damaging**
  Among small to mid-sized German organizations that have experienced a successful infiltration of the corporate network by ransomware, 21 percent reported that they had to cease business operations immediately, and 14 percent lost revenue, both slightly lower than the global average.

- **Ransom demands are not the small business killer – downtime is. Nearly all small to mid-sized businesses impacted by ransomware experienced hours of downtime**
  We found that for 38 percent of the German organizations that were infected with ransomware, the ransom demanded was $1,000 or less, lower than the global average of 55 percent. In fact, only 32 percent of ransom demands of German companies were in excess of $10,000 and only 1 percent were for more than $50,000, but these were significantly higher than the global averages of 14 percent and three percent, respectively. However, our research also found that for 23 percent of impacted organizations, a ransomware infection caused 25 or more hours of downtime, with some organizations reporting that it caused systems to be down for more than 100 hours. The high levels of ransomware-induced downtime for German organizations was higher than the global average.

- **For many German organizations, the source of ransomware is unknown**
  The most common source of ransomware infections in German organizations are related to email use: 32 percent were from a malicious email attachment and 20 percent were from a malicious link in an email. Organizations in Germany are more likely than the global average to know the source of the infection: only 17 percent of German organizations did not know the source of the ransomware infection versus 27 percent globally.

- **Ransomware infections often spread beyond the initial point of infection**
  Our research found that in many ransomware attacks the infection is not limited to a single endpoint, but can spread to others, as well. In fact, in some cases the infection spread to every endpoint on the network. Organizations in Germany were slightly less likely than the global average to see ransomware infections spread to more than just the initial endpoint that was infected, but not every endpoint; but German organizations were more than twice as likely to experience every endpoint on the network become 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 respondents believe that ransomware demands should never be paid (significantly higher in Germany than the global average), while most of the remaining organizations believe they should be paid if the encrypted data is of value to the organization. Only a tiny minority believe that ransom demands should always be paid, and German organizations are less likely to believe they should always be paid than organizations globally.

- **Not paying ransom can result in lost files**
  We found that among German organizations that did not pay the ransom that was demanded of them, 24 percent lost files, significantly lower than the global average of 32 percent.

GERMANY

- **Most organizations give a high priority to addressing the ransomware problem, but many still lack 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 (77 percent of the German organizations surveyed versus 75 percent globally); to investing in resources, technology and funding to address the problem (68 percent compared to 67 percent globally); and to investing in education and training about ransomware for end users (53 percent in Germany and globally).

  Despite these investments, 25 percent of the German 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. However, German organizations indicated that they are significant more confident than the global average in dealing with ransomware.

RANSOMWARE TECHNOLOGY TRENDS

- **Small to mid-sized businesses believe fighting ransomware is more about technology than people**
  When asked if ransomware should be addressed only through technology or only through training, more German organizations believe the former will be more effective in addressing the ransomware problem, which is consistent the global view that technology is more effective. Although the remaining 87 percent of German respondents believe that a mix of technology and training are necessary, these organizations tilt much more toward technology-based approaches as the more effective way to deal with ransomware.

- **Current anti-ransomware technology does not seem to be solving the problem**
  Our research found that organizations have implemented a variety of solutions to address their ransomware concerns, either before or after the fact. These include traditional email security solutions, regular backups to be able to restore to a known good state, network segmentation, and ransomware-specific solutions, either on-premises and/or in the cloud. However, having these defenses in place does not seem to be enough. While more than two in five small to mid-sized German organizations claim to be running anti-ransomware technologies (higher than the global average), 34 percent of those surveyed still experienced a ransomware attack.

ABOUT THIS SURVEY AUDIENCE

The distribution of industries surveyed in Germany is shown in Figure 1. These organizations had a mean of 413 employees and 233 email users.

Figure 1
Distribution of Organizations Surveyed

Industry	%
Financial services/Banking/Insurance	17%
Retail/E-commerce	17%
Engineering/Construction	14%
Government	10%
Manufacturing	9%
Transportation	7%
Food/Agriculture	6%
Healthcare	6%
High tech	3%
Hospitality	2%
Pharmaceutical	2%
Education	1%
Law enforcement	0%
Other	5%

Source: Osterman Research, Inc.

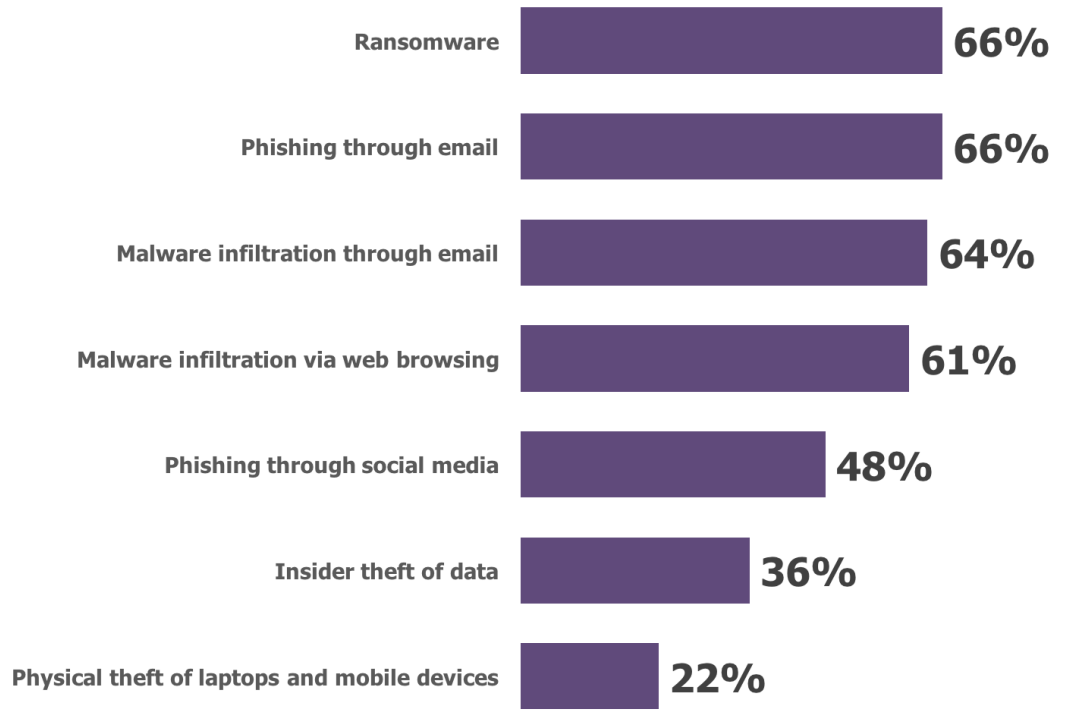
GERMANY

RANSOMWARE IS A CRITICAL PROBLEM

RANSOMWARE IN THE CONTEXT OF OTHER SECURITY THREATS

The ransomware problem has become critical, and the problem is getting worse over time. As shown in Figure 2, ransomware is the most serious problem about which we queried for organizations in Germany, cited by 66 percent of those surveyed as a problem about which they are "concerned" or "extremely concerned", and tied with email phishing as a top concern. 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, with the United States ranking second at 74.2 percent. It is important to note that while ransomware is viewed less seriously in Germany than we discovered across all geographies, it is still a very serious problem for Germany organizations.

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



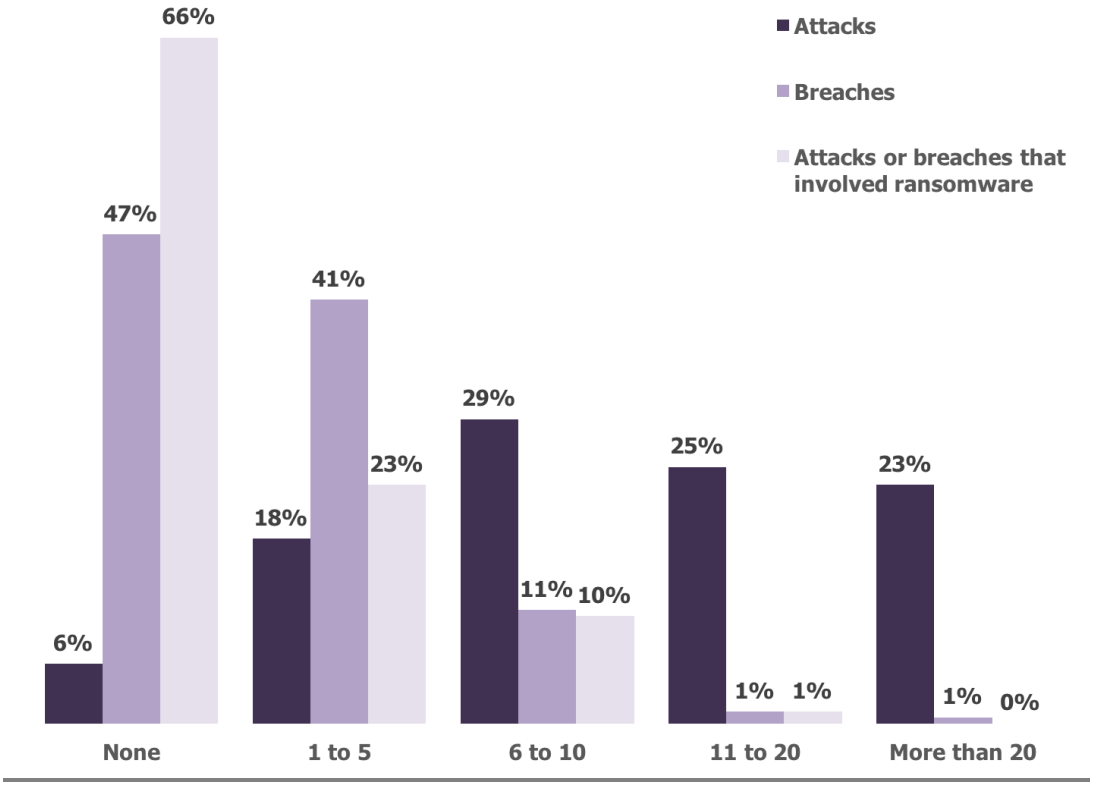
Source: Osterman Research, Inc.

GERMANY

HOW COMMON ARE RANSOMWARE AND OTHER THREATS?

As shown in Figure 3, most organizations in Germany 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 34 percent of German 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 German companies we surveyed actually rank slightly better than the global average: 34 percent of German companies have been victimized over the past year versus 35 percent globally.

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



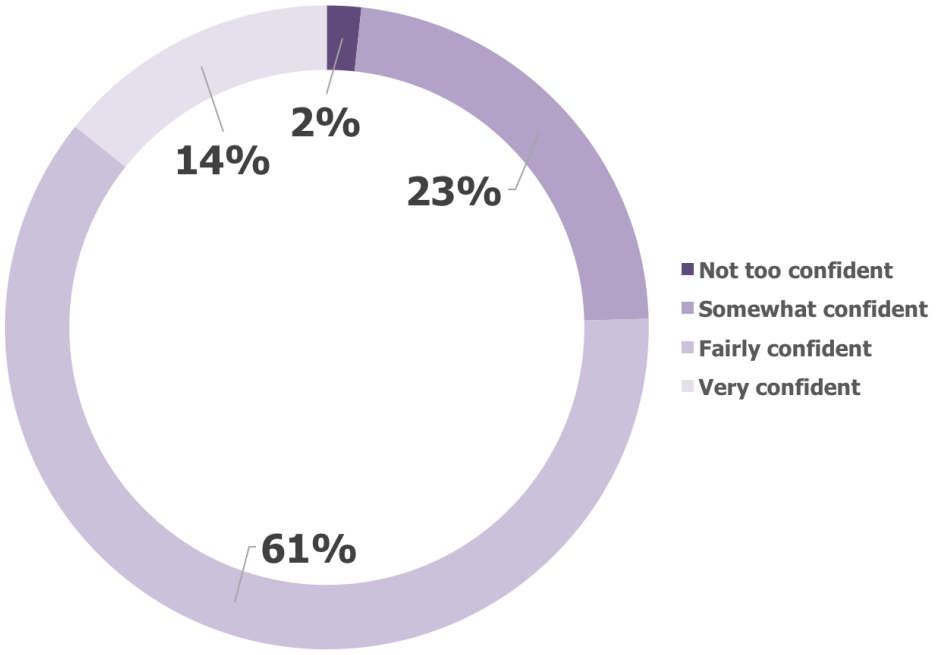
Source: Osterman Research, Inc.

GERMANY

CONFIDENCE IN ADDRESSING THE RANSOMWARE PROBLEM

Organizations' confidence among decision-makers in Germany about their ability to stop a ransomware attack is not very high, but it is higher than the global average. As shown in Figure 4, two percent of organizations has relatively little confidence that they can stop a ransomware attack that has infiltrated their network, and another 23 percent are only "somewhat" confident in their ability to stop such attacks. However, 75 percent of German organizations are "fairly" or "very" confident that it can thwart a ransomware attack, substantially higher than the global average of 54 percent.

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



Source: Osterman Research, Inc.

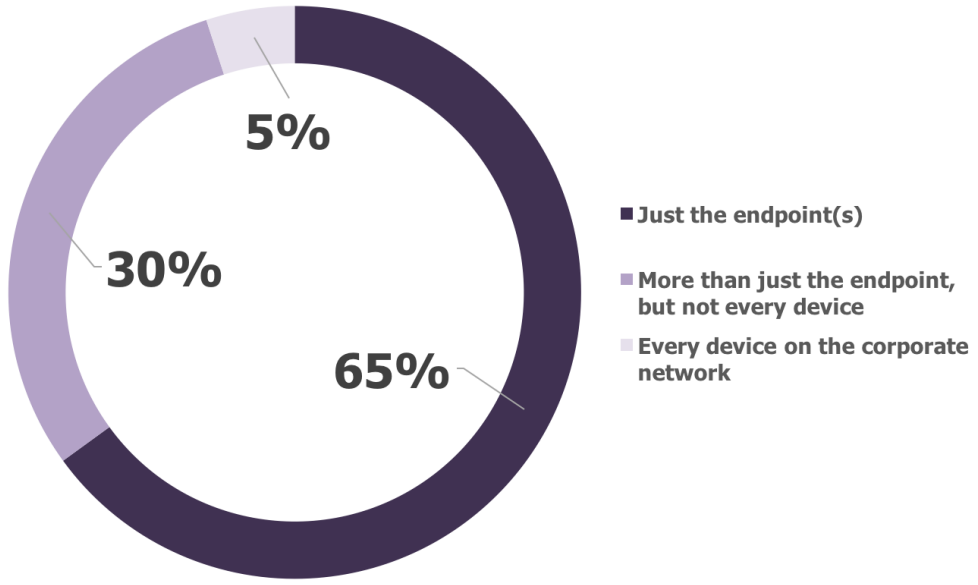
GERMANY

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, 35 percent of these infections spread to other devices, and for five percent of organizations the ransomware infection impacted every device on the network. The spread of ransomware was slightly worse among the German organizations we surveyed compared to the global average. For example, the spread of ransomware to every device on the network was five percent in Germany compared to two percent globally.

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



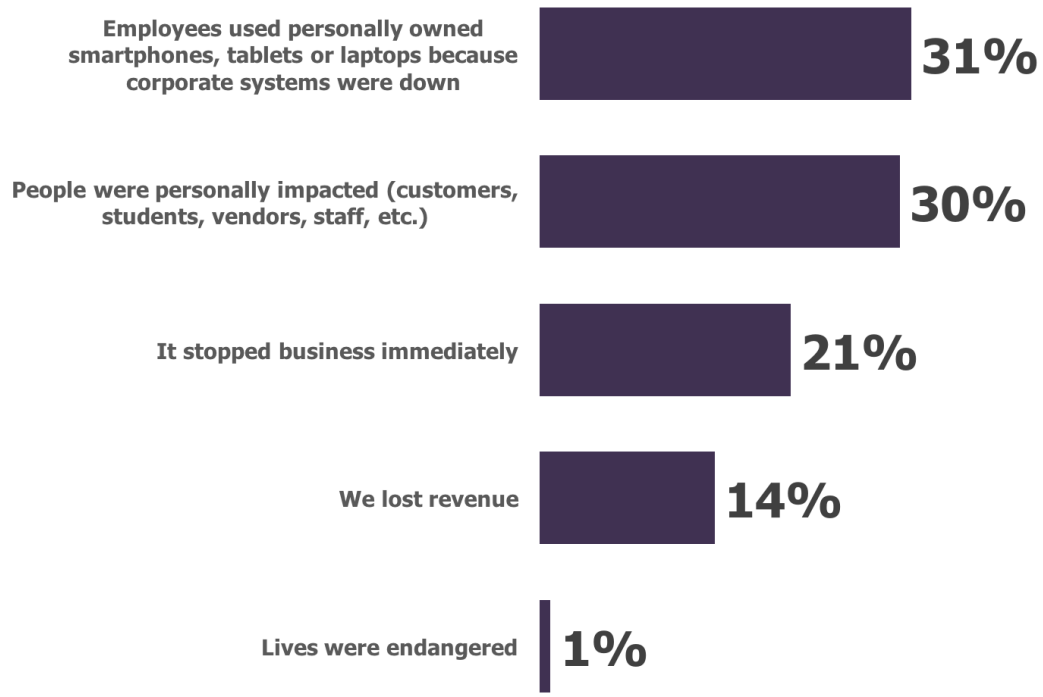
Source: Osterman Research, Inc.

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, whereas this figure was only 50.7 percent for Australian organizations.

GERMANY

Infections from ransomware attacks create a wide range of consequences. As shown in Figure 6, the most significant impact on German organizations was that employees used personally owned platforms when their primary, corporate platform was not available because of ransomware – this was nearly twice the global average of 16 percent. However, the proportion of German companies that experienced an immediate cessation of business and lost revenue was about on par with the global averages we discovered.

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

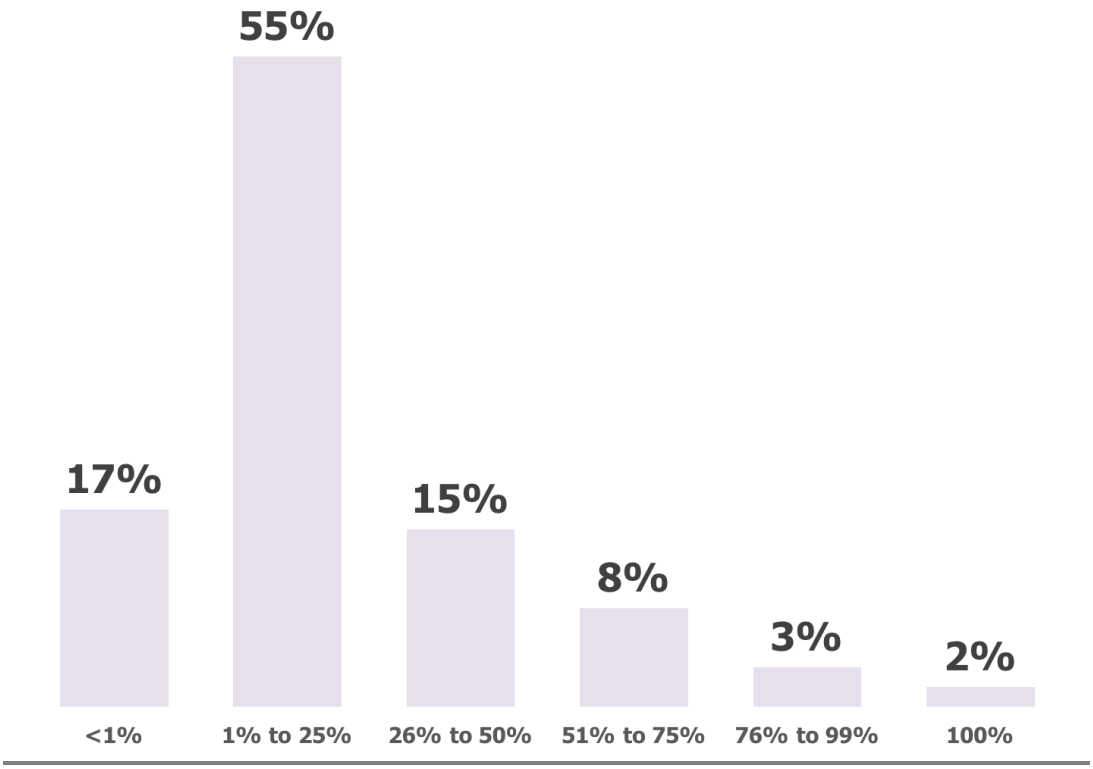


Source: Osterman Research, Inc.

GERMANY

As shown in Figure 7, only about one in six German organizations that fell victim to ransomware had fewer than one percent of their endpoints infected, while 55 percent had up to one-quarter of endpoints infected. However, the remaining 28 percent had more than 25 percent of their endpoints infected. The situation in Germany was slightly worse than it was globally: 28 percent of German organizations had more than one-quarter of their endpoints infected in their most serious ransomware attack versus 26 percent globally.

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



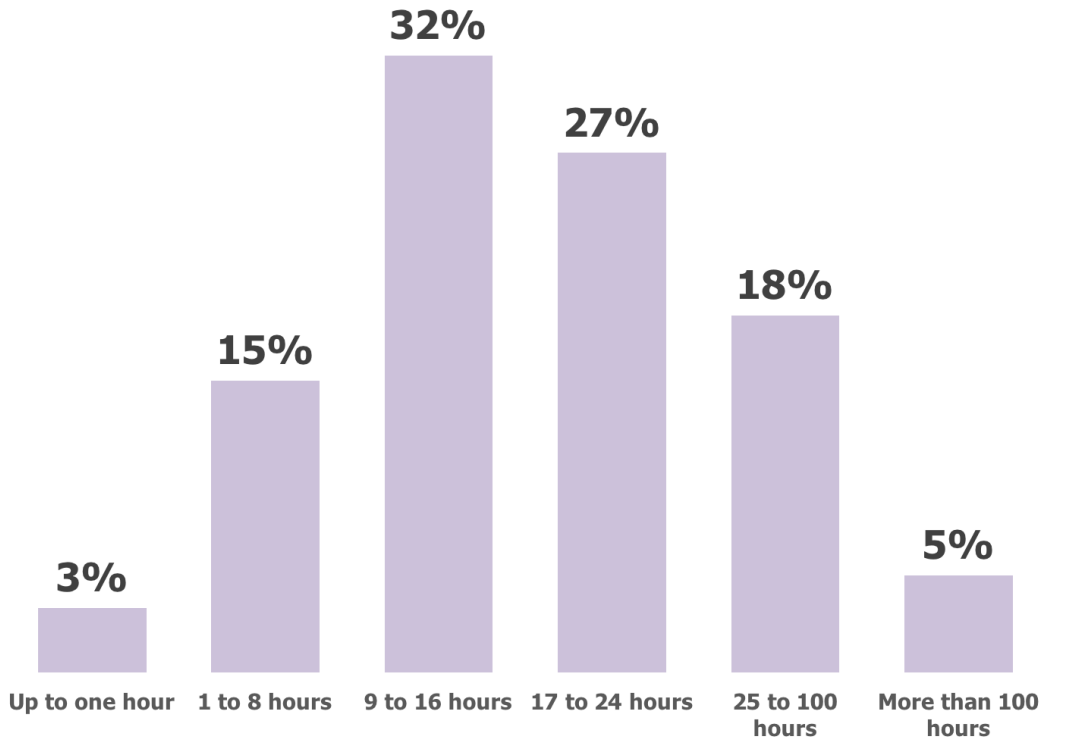
Source: Osterman Research, Inc.

GERMANY

Ransomware-induced downtime is a major consequence for many ransomware infections because an infected endpoint becomes immediately unavailable and remains so for many hours or even days in some cases. 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 three percent of German organizations had minimal downtime resulting from ransomware, but another 15 percent of organizations experienced anywhere from one to eight hours of downtime. However, it gets much worse: 80 percent of organizations infected by ransomware experienced nine or more hours of downtime, with some organizations finding that they were down more than 100 hours because of the infection. The results we obtained for German organizations was worse in some respects compared to the global average: only three percent of German organizations experienced minimal downtime from ransomware infections versus nine percent globally, and five percent of German organizations had in excess of 100 hours compared to just two percent globally.

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



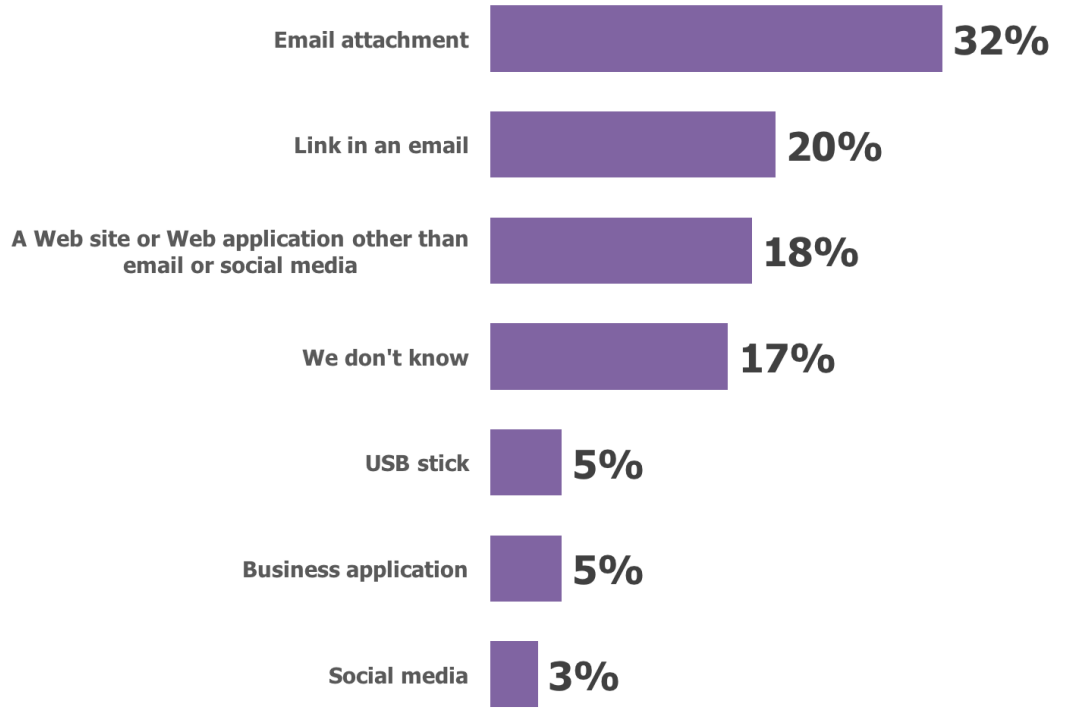
Source: Osterman Research, Inc.

GERMANY

HOW DOES RANSOMWARE ENTER AN ORGANIZATION?

The most commonly cited source of a ransomware infection in German organizations was an email attachment, followed by a malicious link in an email. However, as shown in Figure 9, about one in six organizations simply did not know the source of the most serious ransomware attack that had impacted them. Other sources included a malicious web site or web application, a business application, a social media tool or a USB stick. German organizations were much less likely not to know the source of their most serious ransomware infection: while 17 percent of German organizations did not know the source, 27 percent globally could not identify the source.

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

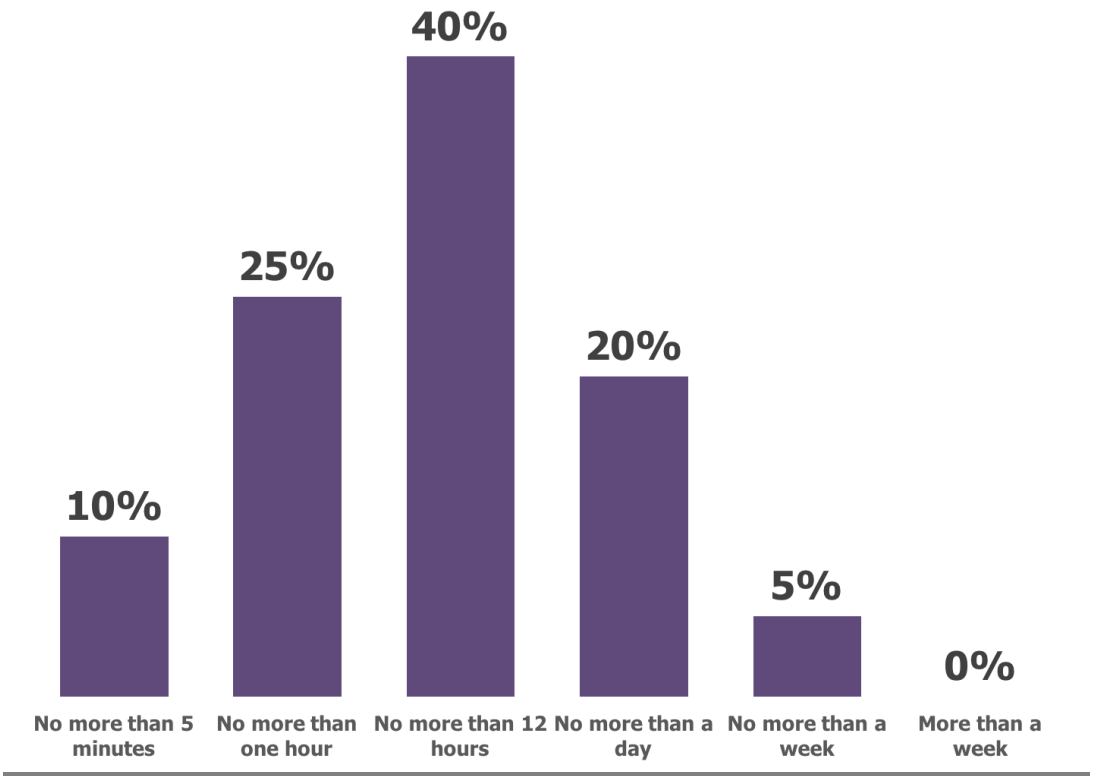


Source: Osterman Research, Inc.

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, 10 percent of German organizations could detect a ransomware infection in five minutes or less, better than the global average of seven percent. Another 25 percent could do so more in no more than one hour after an endpoint was infected, but 65 percent of the German organizations surveyed required many hours or even days before they detected the problem. The results we discovered among organizations in Germany were somewhat worse than the overall global results: while 22 percent of organizations globally took a day or more to detect a ransomware infection, this figure was 25 percent in Germany.

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



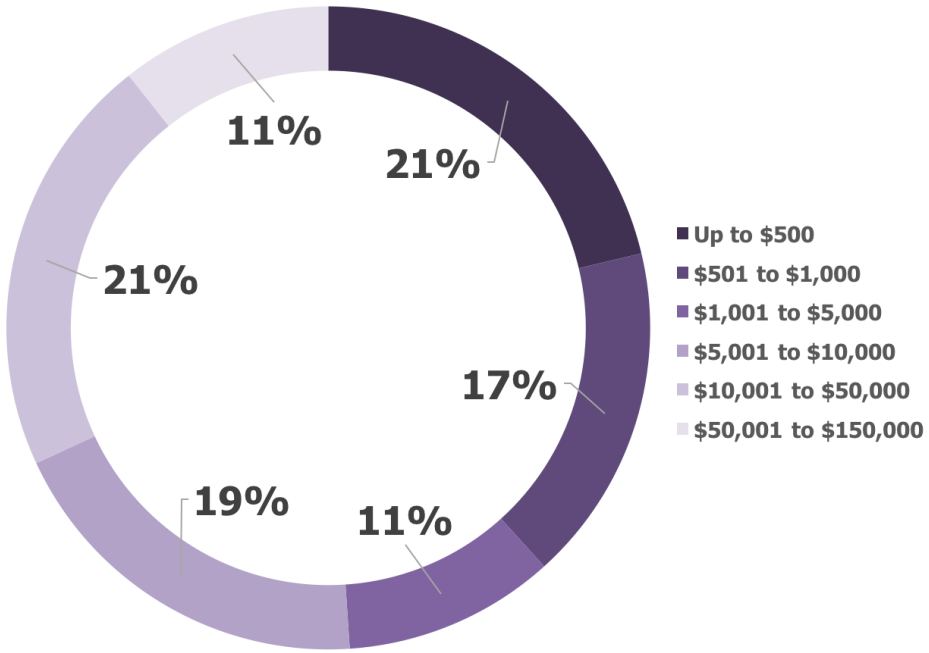
Source: Osterman Research, Inc.

GERMANY

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, 38 percent 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 62 percent asking for more than $1,000 and 11 percent demanding up to $150,000. The results we found for organizations in Germany were substantially worse than the global average: while 14 percent of organizations globally were extorted for more than $10,000, this figure was 32 percent in Germany.

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

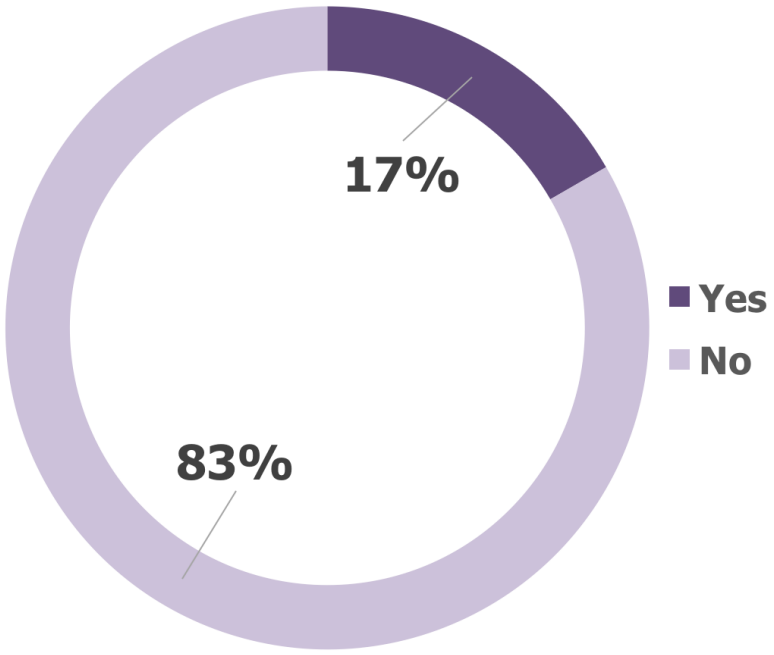


Source: Osterman Research, Inc.

GERMANY

Among German organizations that were infected with ransomware, only about one in six opted to pay the ransomware demands, as shown in Figure 12. However, we found significant variability between the geographies that we surveyed. For example, only 16 percent of French organizations opted to pay the ransom demanded after their most severe ransomware infection (about on par with German organizations' reluctance to pay), but 43 percent of British and 46 percent of Australian organizations opted to do so. Organizations in Germany were significantly less likely to pay ransomware demands than the global average (17 percent versus 28 percent).

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

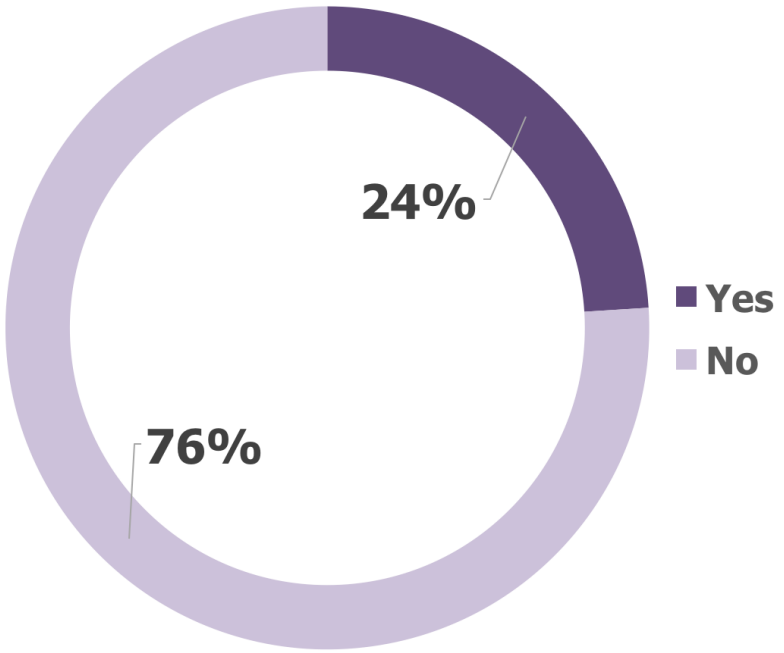


Source: Osterman Research, Inc.

GERMANY

Among German organizations that chose not to pay cyber criminals' ransom demands, about 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, with German organizations losing files less frequently than the global average (24 percent in Germany versus 32 percent globally).

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



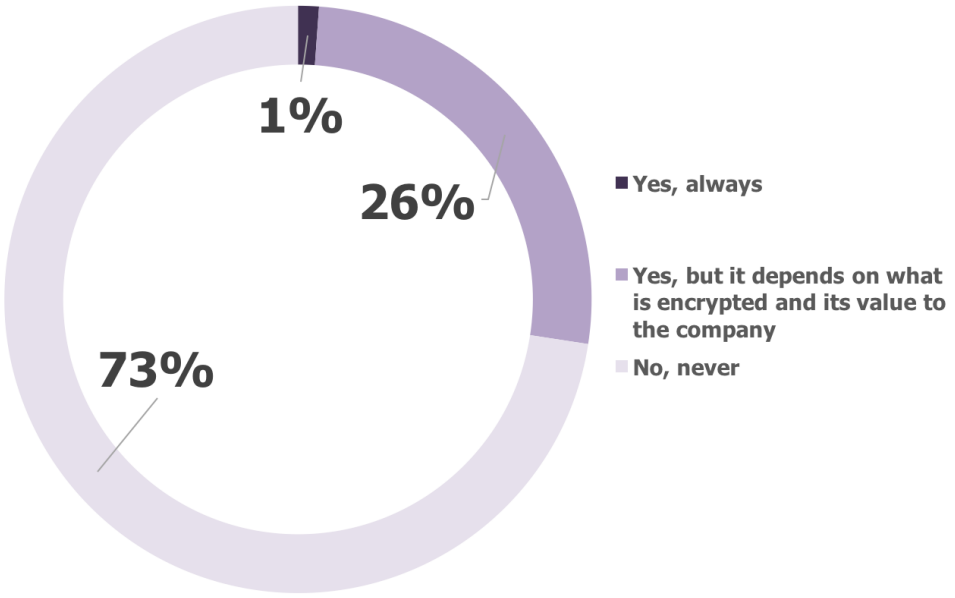
Source: Osterman Research, Inc.

GERMANY

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, the vast majority of organizations in Germany believe, at least in general, that organizations should not pay ransomware demands. At the opposite end of the scale, one percent believe that organizations should always pay the ransom. Interestingly, organizations in Germany are much less likely to believe that organizations should pay ransom demands than is the case for the global average (27 percent in Germany versus 41 percent globally).

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

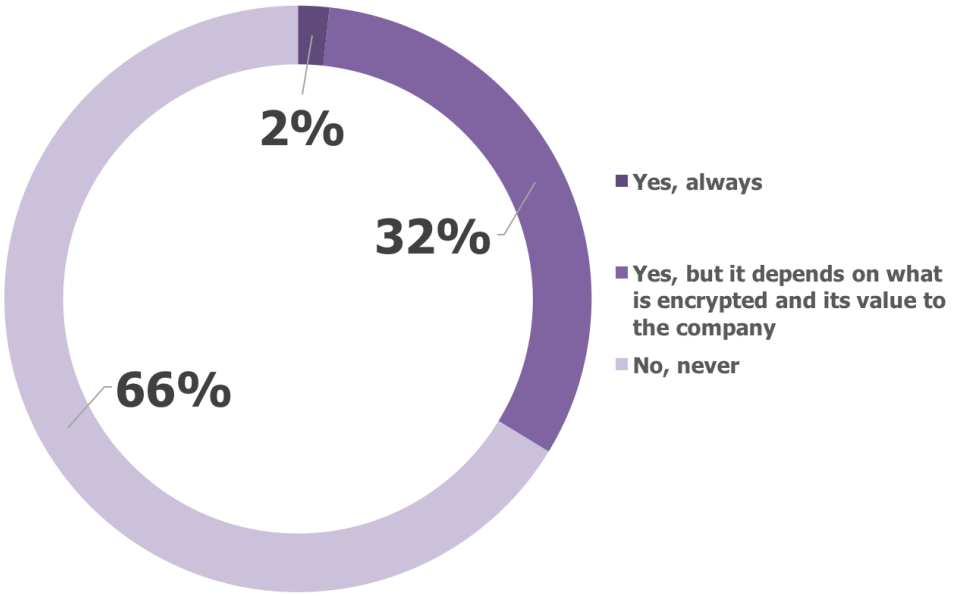


Source: Osterman Research, Inc.

GERMANY

We also asked survey respondents to personalize the decision of whether or not to pay ransom demands. As shown in Figure 15, German organizations are more open to the notion of paying ransom demands when it comes to their own organization than for others. Even so, German organizations are still more reluctant to always pay ransom demands than their global counterparts (two percent in Germany versus three percent globally), and to do so on a case-by-case basis (32 percent in Germany versus 37 percent globally).

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



Source: Osterman Research, Inc.

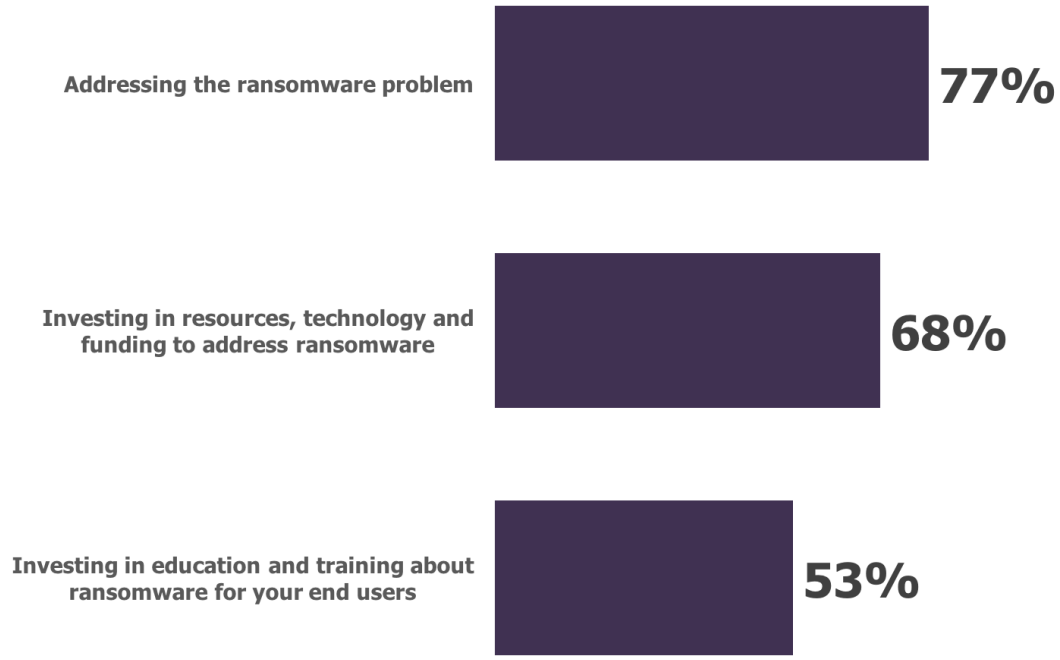
GERMANY

THE IMPORTANCE OF ADDRESSING THE RANSOMWARE PROBLEM

THE NEED TO SOLVE THE RANSOMWARE PROBLEM

Decision makers are mostly in agreement that the ransomware problem needs to be solved and they are addressing it as a high priority. As shown in Figure 16, 77 percent of survey respondents give a "high" or "very high" priority to addressing the ransomware problem in Germany (slightly higher than the global average of 75 percent); 68 percent give investing in resources, technology and funding to address ransomware this high a priority (versus 67 percent globally); and 53 percent consider that investing in user education and training about ransomware needs to be a high or very high priority (the same as the global figure).

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



Source: Osterman Research, Inc.

GERMANY

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, 10 percent of the organizations surveyed believe ransomware can be addressed properly only through a technology-focused approached, while another 39 percent believe that the problem is best addressed mostly using anti-ransomware technology. By contrast, only 21 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

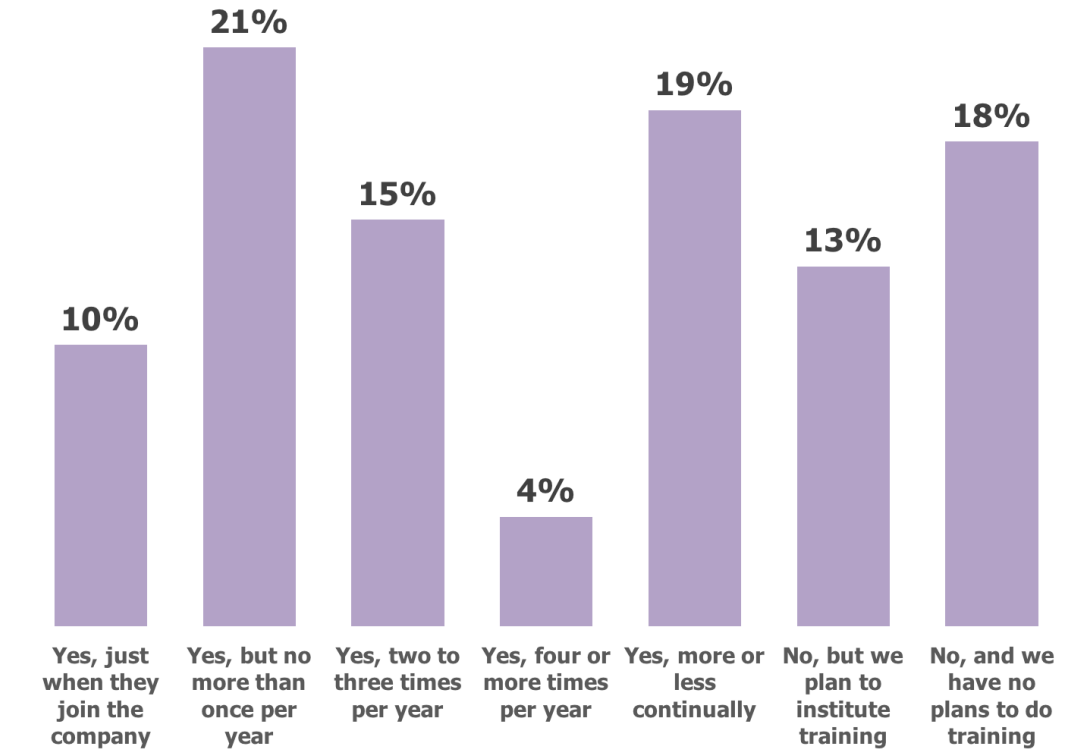
Source: Osterman Research, Inc.

Organizations in Germany take a decidedly more technology-centric approach compared to the global average. For example, while 49 percent of German organizations view ransomware management as mostly technology-focused problem, this figure is only 39 percent globally. Conversely, while only 21 percent of German organizations view dealing with ransomware as mostly about user training, this figure is 30 percent globally.

THE ROLE OF SECURITY AWARENESS TRAINING

In keeping with the lower emphasis for user training discussed above, 31 percent of German organizations do not provide security awareness training that specifically mentions ransomware, as shown in Figure 18. This is substantially higher than the global average of 16 percent. Moreover, while 37 percent of global organizations provide ransomware-focused security awareness training at least once per year or when employees join the organization, this figure is only 31 percent in Germany.

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

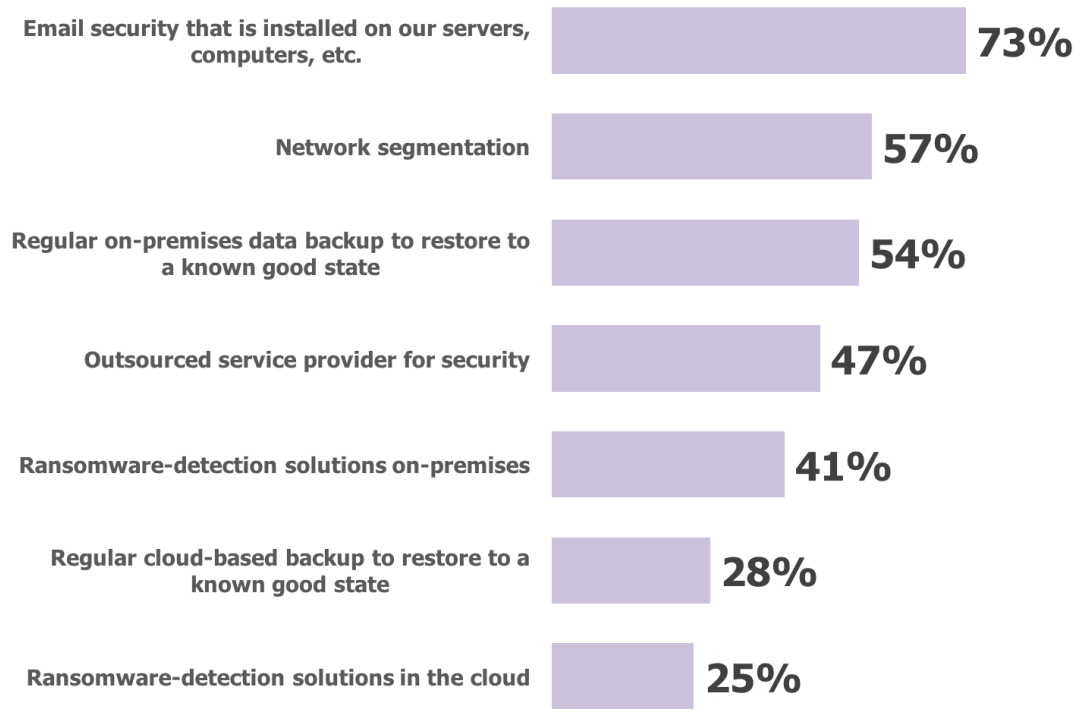


Source: Osterman Research, Inc.

TECHNOLOGIES/PROCESSES IN PLACE TO ADDRESS RANSOMWARE

Most of the German organizations we surveyed have deployed email security to address ransomware and have implemented network segmentation and regular, on-premises backup of data so that they can restore ransomware-infected machines to a known good state as quickly as possible, as shown in Figure 19. Many German organizations also have implemented the use of outsourced security providers, on-premises ransomware-detection solutions, and regular, cloud-based backup capabilities. German firms are less likely to have deployed email security to deal with ransomware (73 percent versus 82 percent globally), but are more likely to have deployed ransomware-detection solutions, both on-premises and in the cloud.

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.

GERMANY