SURVEY REPORT

Understanding the Depth of the Ransomware Problem in the United States

An Osterman Research Survey Report

Published July 2016

Sponsored by

Malwarebytes

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

KEY TAKEAWAYS

- More than 50 percent of corporate decision makers consider ransomware to be a "concern" or "extreme concern".
- Nearly 80 percent of organizations have been the victim of a cyber attack during the past 12 months and nearly 50 percent have been the victim of a ransomware attack.
- The most heavily targeted industries for ransomware are healthcare and financial services.
- Decision makers in U.S. organizations have a relatively low level of confidence in their ability to effectively stop ransomware, and are less confident about the ransomware prevention than their counterparts in Canada, Germany and the United Kingdom. Just four percent of U.S. organizations are "very confident" in their organization's ability to stop ransomware.
- Nearly 80 percent of organizations breached have had high-value data held for ransom. Sixty-eight percent of U.S. companies alone had middle management or above targeted by ransomware.
- Nearly 70 percent of U.S. respondents noted ransomware attacks impacted mid level managers or higher, with 25 percent of incidents attacking senior executives and the C-Suite.
- U.S. organizations are highly committed to solving the ransomware problem: more than 50 percent consider investments in end user ransomware education and technology-based solutions to be a "high" or "very high" priority.
- Ransomware attacks among U.S. organizations tend to be more limited in scope, as measured by the percentage of endpoints impacted, than for the organizations surveyed in other nations.
- Globally, nearly 40 percent of ransomware victims paid the ransom.
- The majority of U.S. organizations believe that training end users and implementing ransomware-focused technologies are equally important.

ABOUT THIS SURVEY REPORT

This report presents the U.S. results of a survey undertaken in the United States, Canada, Germany and the United Kingdom on ransomware and related issues, but with an emphasis on the results from U.S. organizations. The survey was conducted during June 2016 with 165 organizations in the United States, and 125 each in the other nations for a total of 540 surveys completed. In order to qualify for participation in the survey, respondents had to be a CIO, IT manager, IT director, CISO or in a related role; and knowledgeable about security issues within their organization. A total of 21 questions were in included in the online survey. Results from the other surveys are available in separate survey reports. The distribution of industries survey in the U.S. is shown in Figure 1.

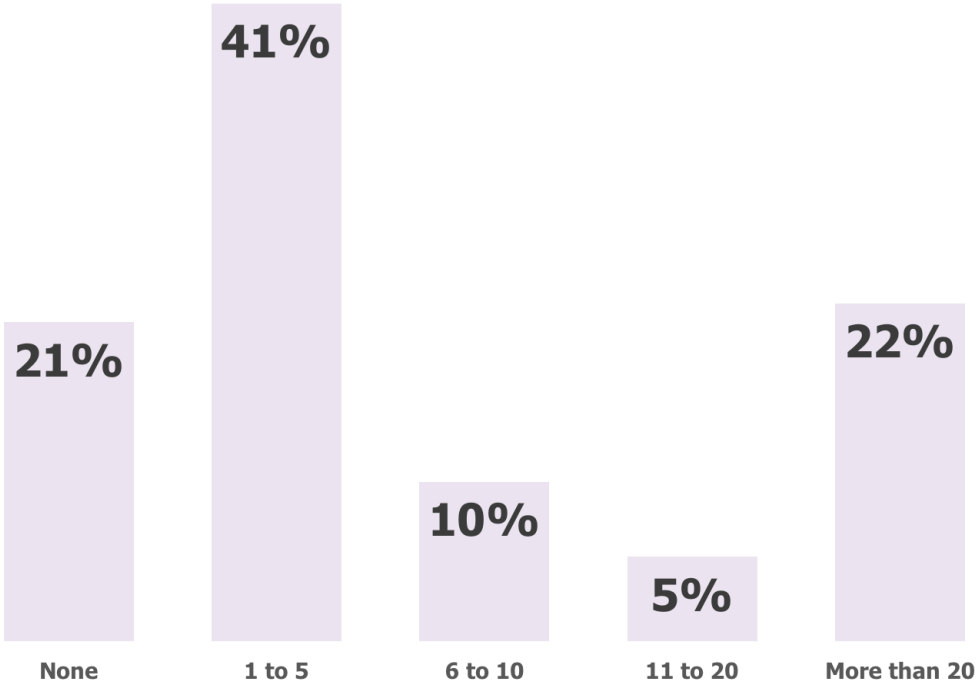
Figure 1
Distribution of Industries Surveyed

Industry	%	Industry	%
Healthcare	18%	Retail/eCommerce	4%
Manufacturing	14%	Engineering/construction	3%
Financial services/banking/insurance	13%	Energy/utilities	2%
High tech	10%	Food/agriculture	2%
Education	8%	Hospitality	1%
Government	8%	Law enforcement	1%
Telecommunications/ISP	4%	Pharmaceutical	1%
Transportation	4%	Other	8%

SURVEY FINDINGS

Four out of five of the U.S. organizations surveyed have suffered a security attack during the previous 12 months, as shown in Figure 2. More than one-quarter of those attacked have experienced more than 20 security attacks during the past year.

Figure 2
Security Attacks During the Previous 12 Months



Source: Osterman Research, Inc.

This data is consistent with other Osterman Research surveys that have shown various types of email- and Web-based attacks on the increase over the past several years.

U.S. organizations are the most attacked among the organizations that we surveyed. For example, as shown in Figure 3, between 28 percent and 35 percent of the organizations in other nations reported no security-related attacks during the previous 12 months versus 21 percent for U.S. organizations. At the other end of the scale, 22 percent of U.S. organizations reported that they had received more than 20 attacks during the previous year compared to between eight percent and 10 percent for organizations in the other nations surveyed.

Figure 3
Security Attacks That Have Occurred During the Previous 12 Months

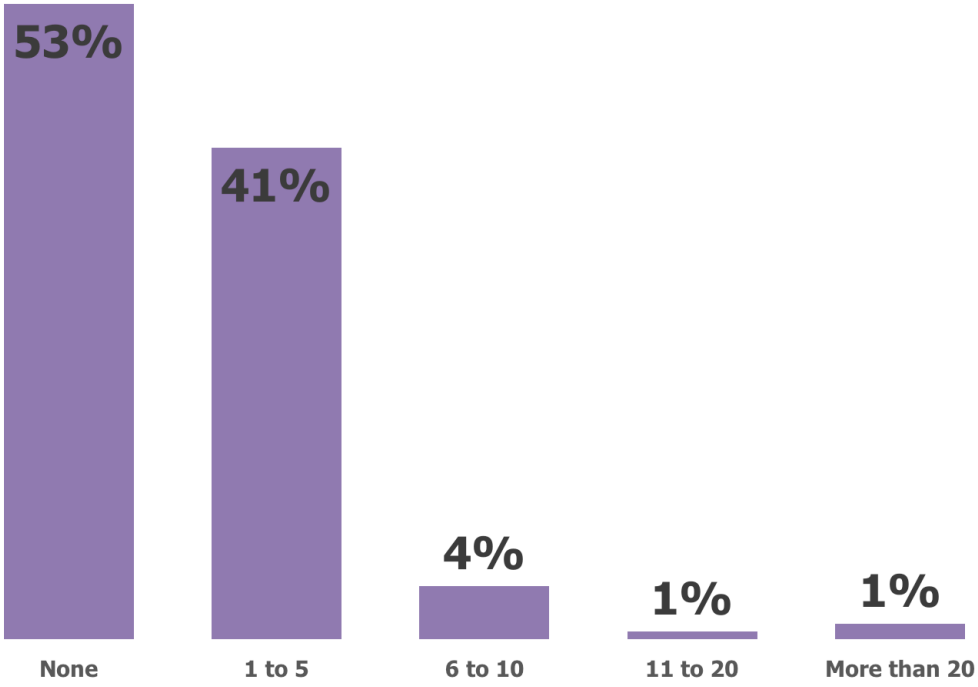
Number of Attacks	USA	Canada	Germany	United Kingdom
None	21%	28%	35%	28%
1 to 5	41%	13%	22%	22%
6 to 10	10%	20%	18%	25%
11 to 20	5%	30%	15%	15%
More than 20	22%	9%	10%	10%

Source: Osterman Research, Inc.

NEARLY ONE-HALF HAVE EXPERIENCED RANSOMWARE ATTACKS

As shown in Figure 4, nearly one-half of the organizations surveyed have experienced a ransomware attack during the past 12 months. Among the organizations that have experienced such an attack, the vast majority has encountered comparatively few of them – a maximum of five. However, almost 10 percent suffered many more attacks, in some cases in excess of 20.

Figure 4
Ransomware Attacks During the Previous 12 Months



Source: Osterman Research, Inc.

Our research found that Canadian and German organizations experience significantly fewer ransomware attacks relative to U.S. organizations, but that those in the United Kingdom experience ransomware attacks to a slightly greater degree – 54 percent of organizations in the United Kingdom have experienced ransomware attacks compared to 47 percent in the United States, as shown in Figure 5. While this may seem to indicate that the ransomware problem is worse in the United Kingdom, we believe that some of the difference may be attributable to differences in the sample population between the two regions. There was a higher proportion of financial services and related firms in the United Kingdom sample, which may have skewed the results slightly higher.

Figure 5
Ransomware Attacks That Have Occurred During the Previous 12 Months

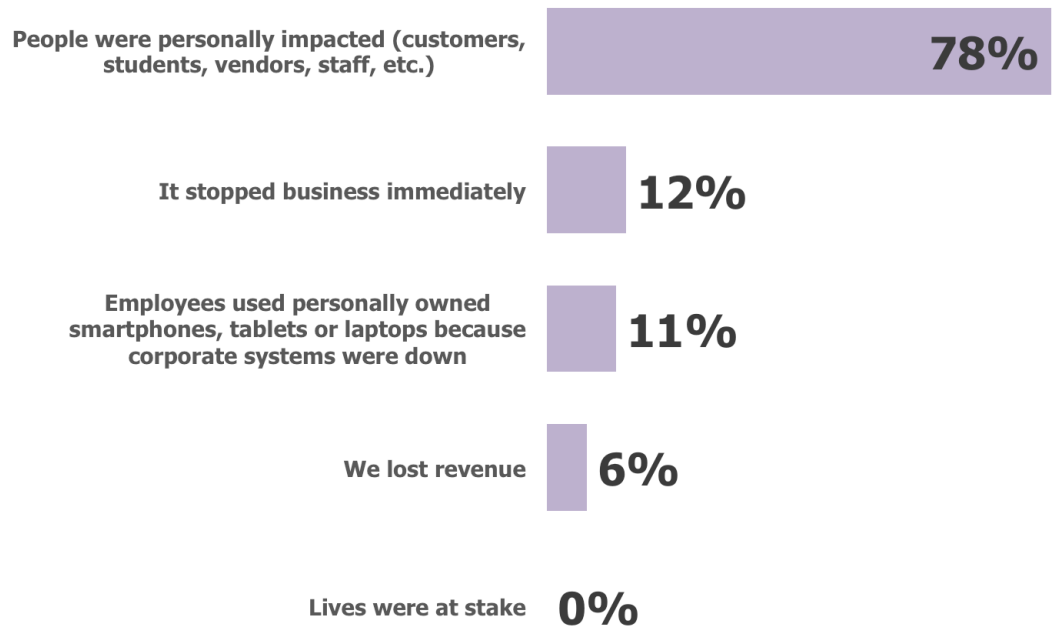
Number of Attacks	USA	Canada	Germany	United Kingdom
None	53%	65%	82%	46%
1 to 5	41%	27%	18%	42%
6 to 10	4%	7%	0%	8%
11 to 20	1%	1%	0%	3%
More than 20	1%	0%	0%	1%

Source: Osterman Research, Inc.

THE IMPACT OF RANSOMWARE CAN BE SEVERE

The impact of ransomware was significant among organizations that were infected – indicating that high value data was compromised. Globally, 34 percent of ransomware attacks caused organizations to lose revenue due to the inability to access encrypted files. In the U.S., six percent of companies reported losing revenue, as shown in Figure 6. Twelve percent of companies in the U.S. had to stop business immediately upon discovering the ransomware attack.

Figure 6
Values of the Files That Were Encrypted



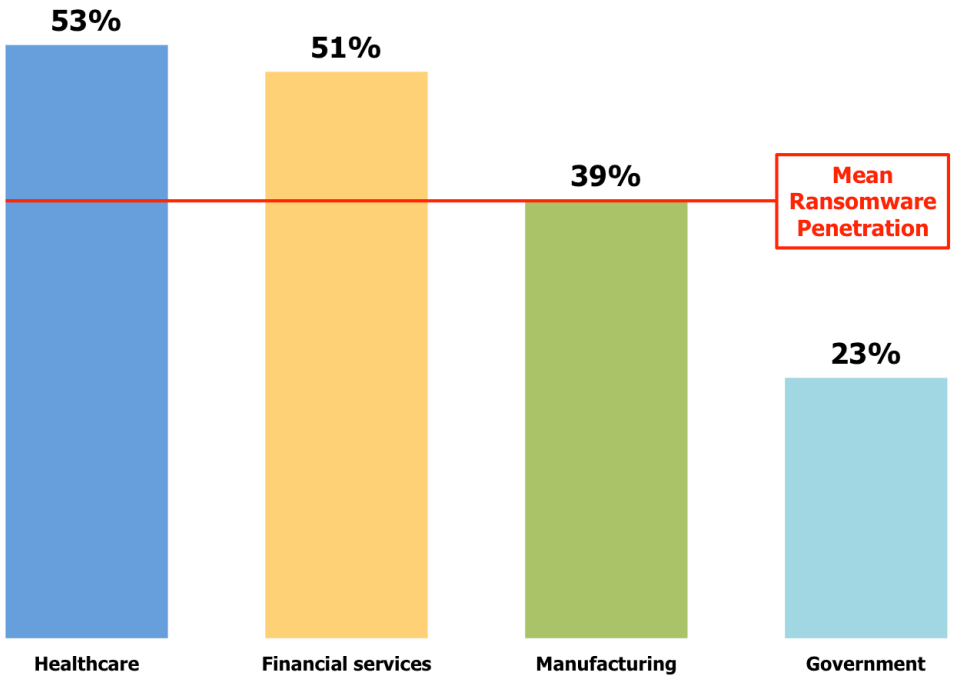
Source: Osterman Research, Inc.

The impact of ransomware in the United States was significantly less than in the other nations we surveyed. For example, only 12 percent of U.S. organizations reported that ransomware "stopped business immediately", compared to Germany (13 percent), the United Kingdom (24 percent) and Canada (25 percent). While U.S. organizations had the greatest level of "personal" impact from ransomware (customers, students, vendors, staff, etc.), the U.S. also had the lowest impact from ransomware on corporate revenue.

RANSOMWARE PENETRATION VARIES BY INDUSTRY

We included a wide range of industries across the various geographies in which the survey was conducted, but the top four industries surveyed were financial services/banking/insurance, manufacturing, government and healthcare, which together represented 49 percent of the surveys conducted. As shown in Figure 7, healthcare and financial services were the leading industries attacked with ransomware, both of which were targeted well above the average ransomware penetration rate of 39 percent.

Figure 7
Ransomware Attacks That Have Occurred During the Previous 12 Months
Includes data from the four geographies surveyed

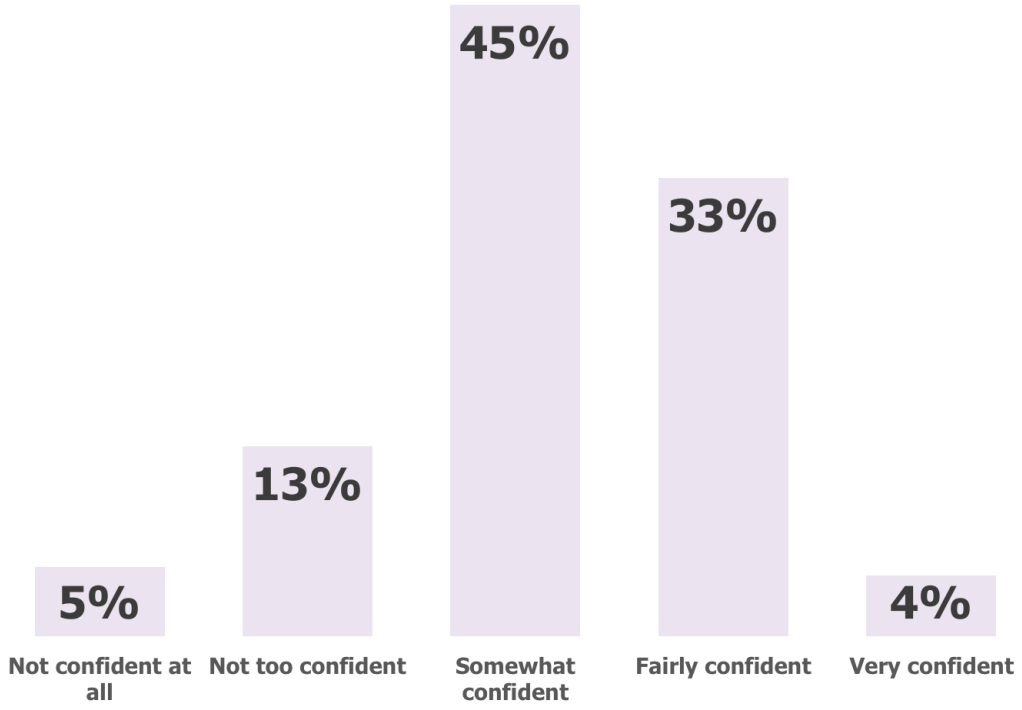


The fact that healthcare and financial services were the most vulnerable to ransomware attacks comes as no surprise. These industries are among the most dependent on access to their business-critical information, which makes them prime targets for ransomware-producing cyber criminals. Cyber criminals, hoping that organizations will not have ransomware detection technologies in place or will not have recent backups of their data from which they can recover, are more likely to target organizations in these industries, particularly for highly targeted, spearphishing-like attacks.

MISPLACED CONFIDENCE FOR DEFEATING RANSOMWARE

Only four percent of organizations are "very confident" of their ability to stop ransomware, as shown in Figure 8. Seventy-eight percent expressed that they were somewhat or fairly confident, despite the fact that nearly 80 percent of organizations have been the victim of a cyber attack during the past 12 months and nearly 50 percent have been the victim of a ransomware attack. Nearly one in five organizations are either not at all confident or only minimally confident in their organization's ability to deal appropriately with ransomware.

Figure 8
Confidence in the Ability to Stop Ransomware



Source: Osterman Research, Inc.

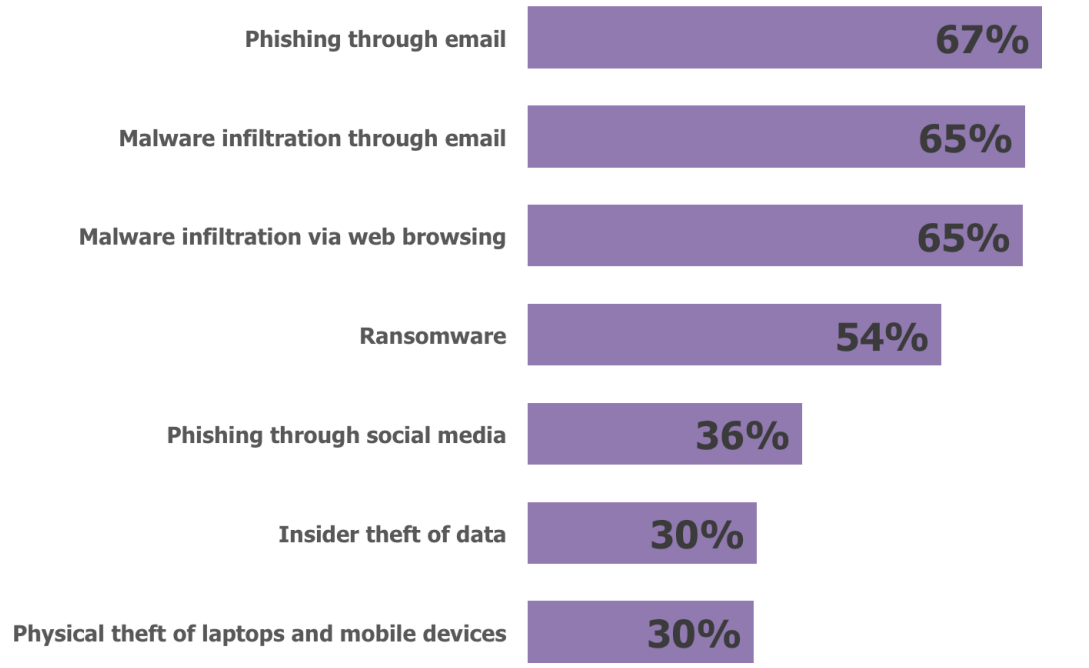
Interestingly, U.S. organizations had the lowest level of confidence in their ability to stop ransomware attacks. For example, the highest response for "not confident at all" was among U.S. organizations (other nations ranged between one percent and three percent), while U.S. organizations also expressed the lowest level of "very confident" responses (other nations ranged from 14 percent to 21 percent). We attribute this somewhat more pessimistic ransomware-related worldview to two things:

- First, U.S. organizations face significantly higher levels of security-related attacks than organizations in the other nations surveyed, as well as a significant level of ransomware attacks.
- Second, somewhat ironically, while U.S. organizations tend toward the view that training end users about ransomware detection and prevention is an effective method for dealing with the problem, U.S. organizations tend to offer less ransomware-related training than organizations in other nations. For example, while between six percent and 23 percent of organizations in Canada, Germany and the United Kingdom currently do not offer ransomware-related training for their end users, this figure is 41 percent among organizations in the United States.

RANSOMWARE IS A KEY AREA OF CONCERN

Ransomware is a serious concern for U.S.-based organizations – as shown in Figure 9, more than one-half are either concerned or extremely concerned about ransomware. However, issues like phishing and malware infiltration through email, as well as malware infiltration through Web browsing, are more serious concerns.

Figure 9
Concerns About Security-Related Problems
% Responding Concerned or Extremely Concerned



Source: Osterman Research, Inc.

While ransomware is the fourth highest security-related concern about which we queried in the survey of U.S. organizations, the level of concern about ransomware is higher in the U.S. than in the other nations we surveyed. For example, 50 percent of organizations in the United Kingdom are concerned or extremely concerned about ransomware, but this figure drops to 32 percent in Canada and a mere 12 percent in Germany, as shown in Figure 10.

Figure 10
Concerns About Various Security-Related Threats

Number of Attacks	USA	Canada	Germany	United Kingdom
Phishing through email	67%	29%	26%	43%
Malware infiltration via web browsing	65%	33%	23%	46%
Malware infiltration through email	65%	44%	43%	53%
Ransomware	54%	32%	12%	50%
Phishing through social media	36%	17%	14%	23%
Physical theft of laptops and mobile devices	30%	5%	4%	10%
Insider theft of data	30%	10%	5%	34%

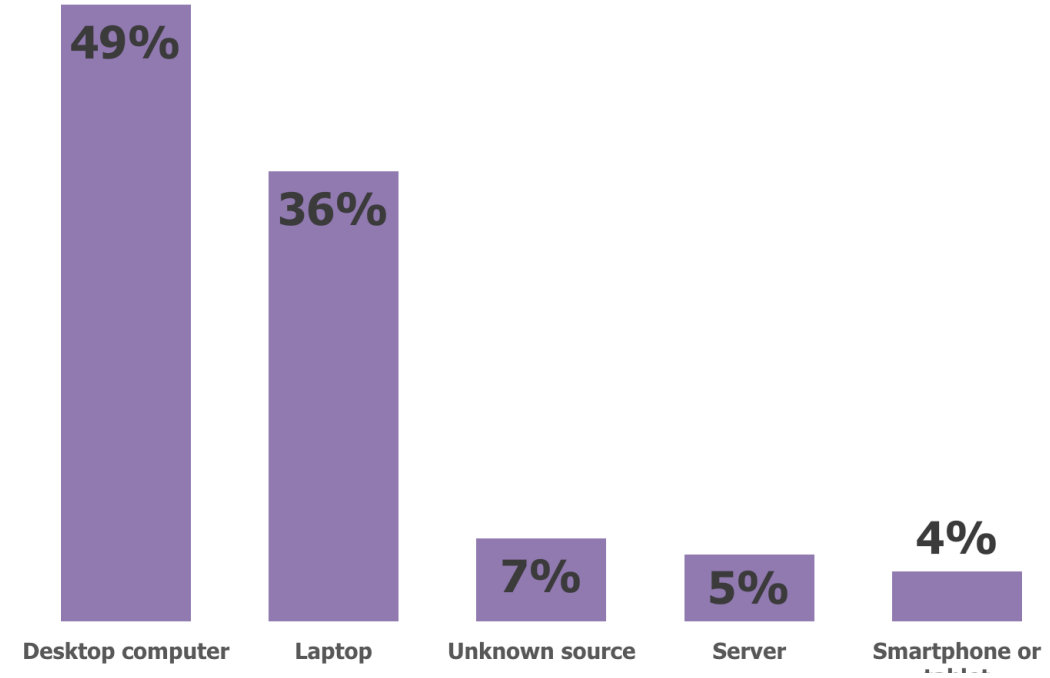
Source: Osterman Research, Inc.

It is important to note, however, that U.S. organizations are more concerned about security across the board than their counterparts in the other nations in which we conducted this survey. For example, the percentage of those in the United States expressing concern or extreme concern about the various security-related problems on which we surveyed was highest in the U.S. for every category. Moreover, the average percentage for the seven categories of security problems was 50 percent in the U.S. compared to 37 percent in the United Kingdom, 24 percent in Canada, and only 18 percent in Germany.

DESKTOPS AS AN INGRESS POINT FOR RANSOMWARE

Interestingly, among organizations that have experienced a ransomware attack, roughly one-half have encountered the attack through a desktop computer, where enterprise security controls and policies would be presumed to be strongest. Laptop computer was the second most common ingress point, as shown in Figure 11. Mobile devices and servers are not common entry points for ransomware, but one in 14 organizations is not sure of the source.

Figure 11
Physical Locations in Which Ransomware Entered the Organization



Source: Osterman Research, Inc.

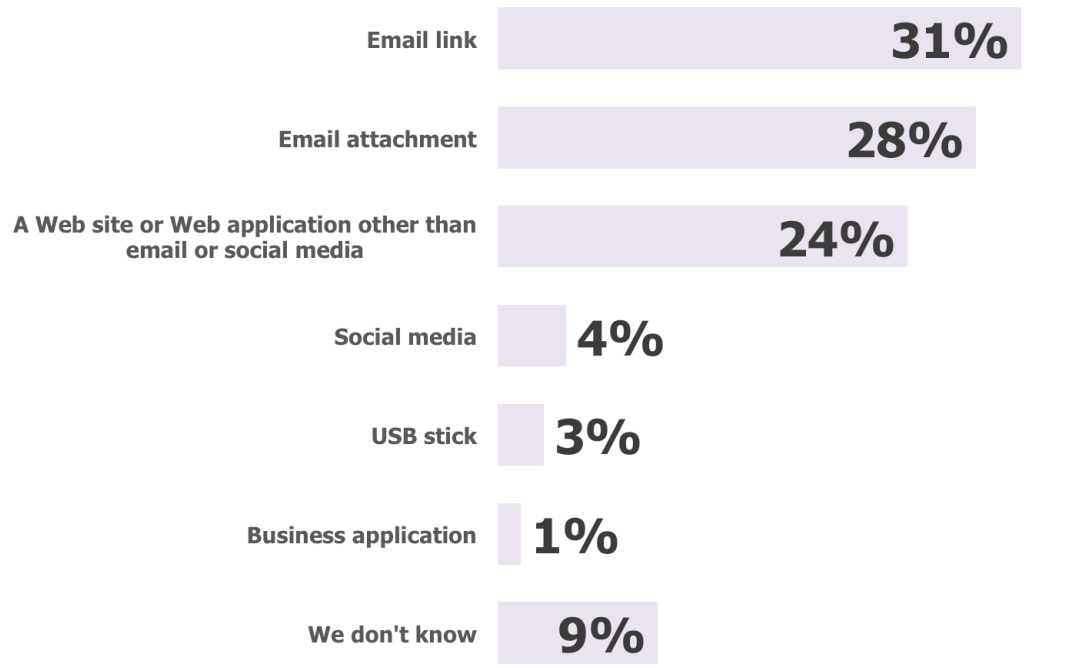
Interestingly, U.S. organizations reported the lowest level of malware infiltration from desktop computers (49 percent in the U.S. compared to 49 percent to 74 percent in the other nations surveyed), but the highest level of infiltration from laptops (36 percent in the U.S. versus zero percent to 16 percent in the other nations). This resulted in a higher combined total for desktops and laptops in the United States (84 percent) compared to the other nations surveyed (which ranged from 66 percent to 73 percent).

Part of this difference may be attributable to the fact that there are simply more targets of opportunity for ransomware perpetrators in the United States. For example, approximately 39 percent of all personal computers sold in 2015 were in the United States compared to 25 percent in Europe[1], despite the fact that Europe's population is more than twice that of the United States; and that sales of laptops worldwide are significantly higher than for desktops[2]. That said, unknown sources of ransomware are significantly higher in Canada (16 percent), Germany (13 percent) and the United Kingdom (22 percent) than in the United States (7 percent).

EMAIL IS A PRIMARY THREAT VECTOR FOR RANSOMWARE

As a corollary to the point above, email links and attachments are the primary ingress point for ransomware, as shown in Figure 12. Other common entry points are non-email and non-social media Web sites or Web applications, but in one out of 11 organizations decision makers imply don't know the applications by which ransomware entered the organization.

Figure 12
Applications by Which Ransomware Entered the Organization



Source: Osterman Research, Inc.

Germany (61 percent) and the United States (59 percent) both see the highest level of ingress for ransomware through email, either through email attachments or malicious links in email messages. Email is much less common in the United Kingdom (39 percent) as an entry point for ransomware and in Canada (30 percent). By contrast, business applications are a much more common method for

[1] http://www.statisticbrain.com/computer-sales-statistics/
[2] http://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/

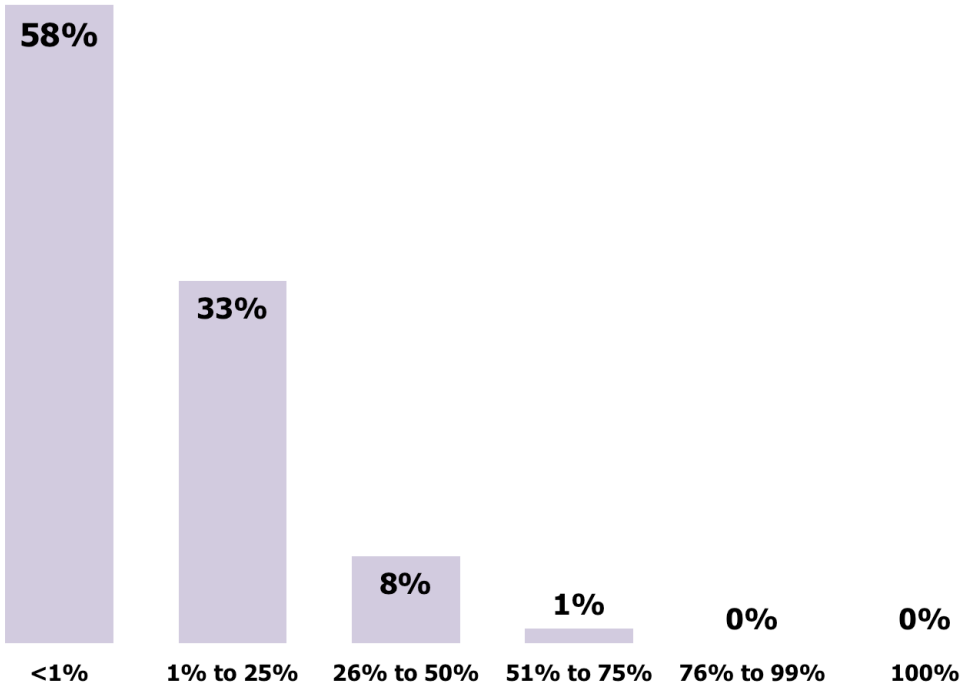
ransomware infiltration in Canada than in the other nations in which we surveyed, accounting for only 1.3 percent of infiltrations in the United States.

A possible explanation for Canada's much lower impact from email as a threat vector for ransomware may be attributable to the Canadian Anti-Spam Law (CASL) that went into effect on July 1, 2014. A Cloudmark report from the first quarter of 2015 found that Canadians are receiving significantly less email than they were before CASL went into effect, even though much of this decline is in legitimate email traffic, not spam. As noted in the Cloudmark report, "While CASL has been ineffective in preventing the professional spammers promoting bootleg pharmaceuticals, diet pills and adult services, it has stopped unscrupulous email marketers from growing their mailing lists by co-marketing or easy-to-miss opt-out checkboxes." While difficult to assess at this point, CASL may have had the unintended effect of reducing the amount of ransomware entering Canadian organizations by virtue of the fact that it has reduced total email volume.

FORTY-TWO PERCENT OF ATTACKS WERE SUCCESSFUL IN IMPACTING MORE THAN A SINGLE ENDPOINT

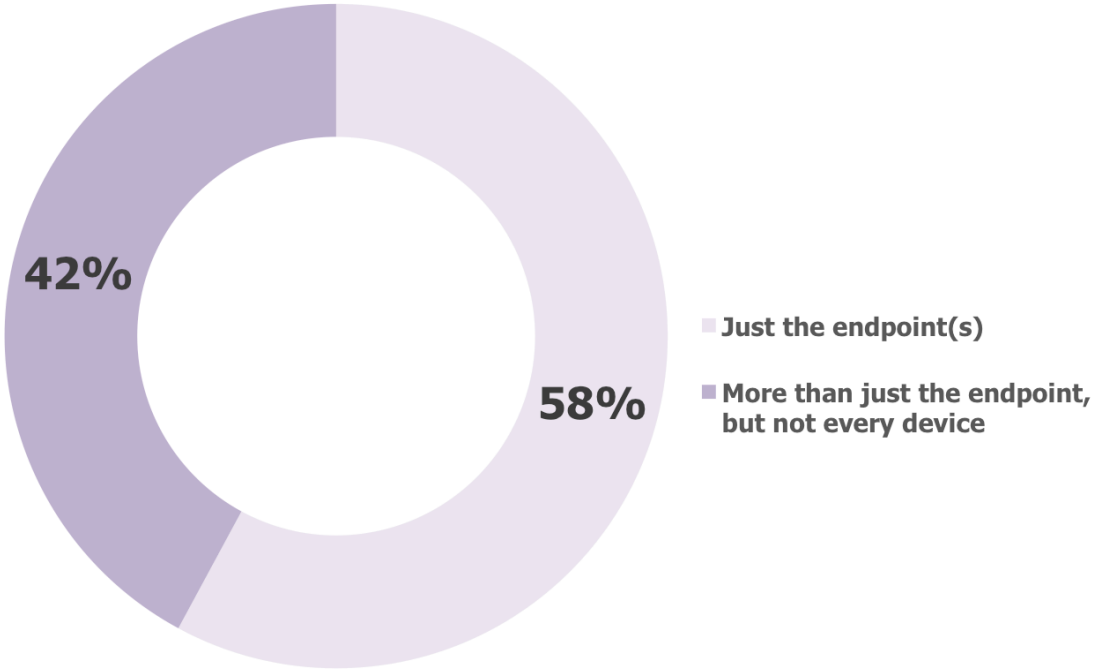
As shown in Figures 13 and 14, more than two in five ransomware attacks were successful in impacting more than a single endpoint, with nearly 10 percent of the attacks affecting more than one-quarter of the endpoints.

Figure 13
Proportion of Endpoints to Which Ransomware Attacks Spread



Source: Osterman Research, Inc.

Figure 14
Endpoints Impacted by Ransomware Attacks



Source: Osterman Research, Inc.

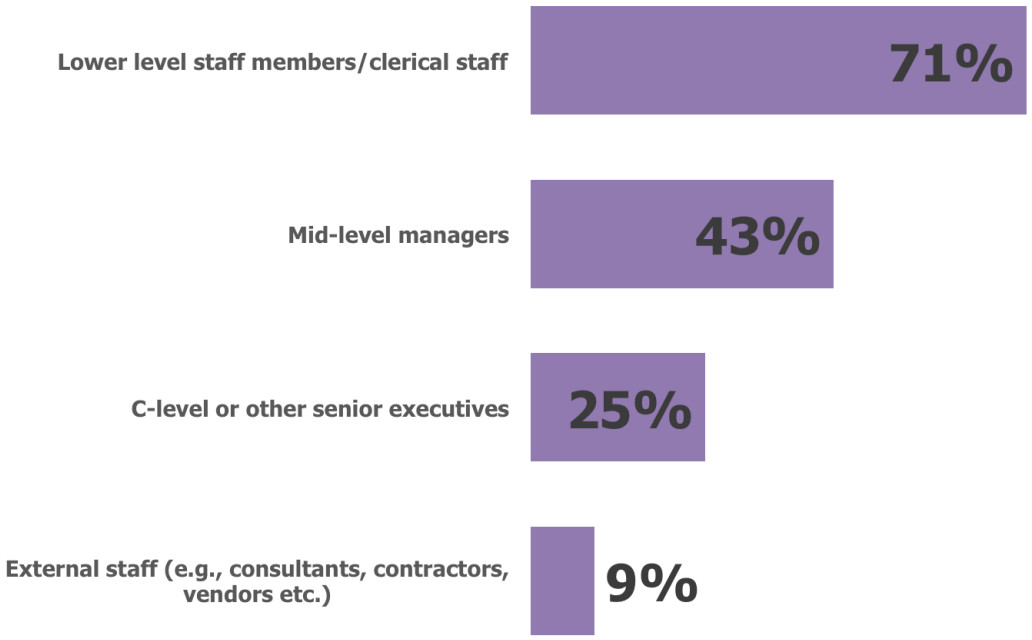
There is a significant difference between organizations in the United States and those in the other nations we surveyed in the context of how widespread ransomware attacks become once they gain a foothold. For example, while 58 percent of U.S. organizations report that fewer than one percent of endpoints become infected as the result of a ransomware attack, these figures range from only four percent to 17 percent in the other nations surveyed. By contrast, those reporting ransomware-penetration rates from 26 percent to 75 percent are only nine percent of the total for U.S. organizations compared to anywhere from 17 percent to 41 percent in the other nations surveyed. In fact, our research found that 10 percent of organizations in the United Kingdom report that all of their endpoints were affected in their most serious ransomware attack.

The much more limited spread of ransomware infection in the United States may at least partially explain why U.S. organizations are much less willing to pay the ransom demanded after an infection: simply put, U.S. organizations have less to lose by not paying, since far fewer endpoints are impacted by ransomware and less data will be lost as a result.

MID-LEVEL AND EXECUTIVES ARE DISPROPORTIONATELY AFFECTED

The majority of U.S. organizations that have experienced a ransomware attack have seen the primary impact on their lower level staff members, such as clerical staff who have access to computing resources, as shown in Figure 15. However, mid-level managers and senior executives are disproportionately affected by ransomware given their substantially smaller numbers. For example, if we assume that in the typical organization only five percent of the employees are senior executives, then the fact these individuals represent 25 percent of the victims of ransomware means that they are impacted far more often than lower level staff members.

Figure 15
Roles Impacted by Ransomware Attacks



Source: Osterman Research, Inc.

U.S. organizations see a much greater impact from ransomware on lower level staff members than do organizations in the other nations in which we surveyed (71 percent in the United States compared to 14 percent to 29 percent in the other nations). However, U.S. organizations also see much greater impacts from ransomware on C-level and other senior executives (25 percent in the United States compared to six percent to 15 percent in the other nations surveyed.) In fact, the proportion of employees impacted from ransomware in the United States is much higher: a mean of 37 percent across job functions compared to 23 percent in the United Kingdom, 14 percent in Canada and nine percent in Germany, as shown in Figure 16.

Figure 16
Roles That Have Been Impacted by Ransomware

Number of Attacks	USA	Canada	Germany	United Kingdom
Lower level staff members/clerical staff	71%	23%	14%	29%
Mid-level managers	43%	22%	13%	42%
C-level or other senior executives	25%	8%	6%	15%
External staff (e.g., consultants, contractors, vendors etc.)	9%	2%	2%	7%

Source: Osterman Research, Inc.

The fact that ransomware is impacting such a large proportion of lower level staff members implies that cyber criminals are using ransomware in untargeted, widespread attacks in the U.S. Because

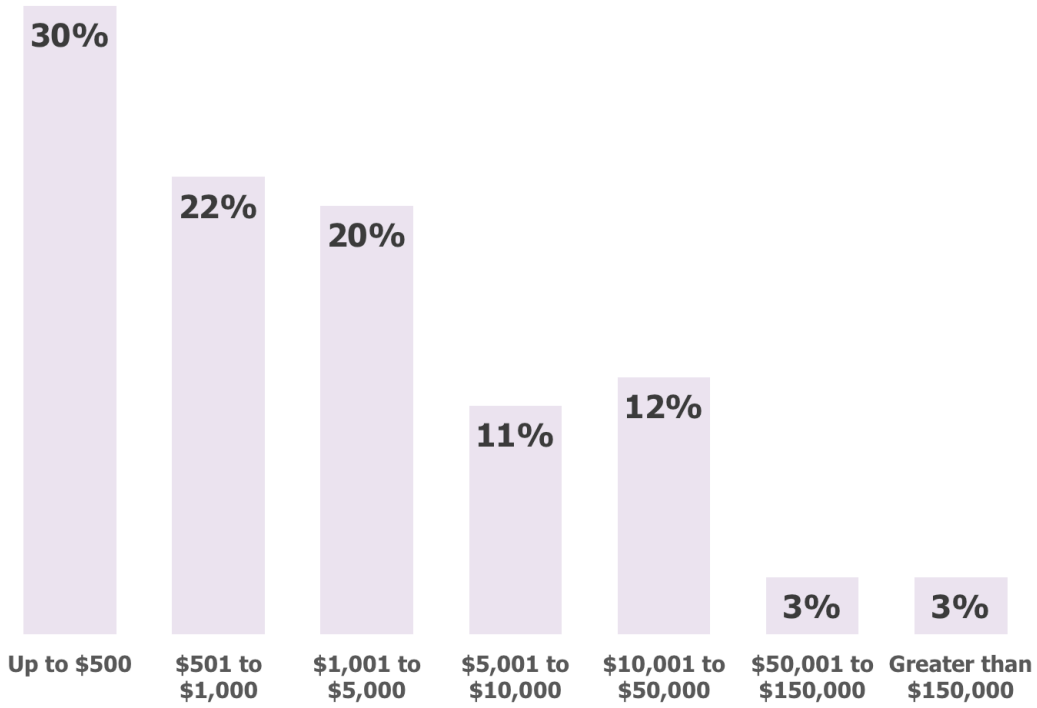
ransomware capabilities can be procured for relatively small sums, this opens the market to a wide range of "amateur" cyber criminals who are pumping out ransomware exploits with spam-like frequency. As noted in a December 2015 *Business Insider* article about ransomware-as-a-service, "Ransomware *as a service* is a variant of ransomware designed to be so user-friendly that it could be deployed by anyone with little cyber know-how. These agents simply download the virus either for free or a nominal fee, set a ransom and payment deadline, and attempt to trick someone into infecting his or her computer. If the victim pays up, the original author gets a cut — around five percent to 20 percent — and the rest goes to the 'script kiddie' who deployed the attack.[3]"

However, this also demonstrates that cyber criminals are targeting C-level executives and middle managers in an attempt to score large ransomware payments. We see this trend continuing as the ransomware "industry" bifurcates and seeks both mass market and high value victims.

RANSOMWARE DEMANDS REFLECT DIVERSITY OF ATTACKS

The amounts demanded by ransomware perpetrators reflects a diversity of attacks styles and types. As shown in Figure 17, nearly one-third of those victimized by ransomware have faced demands of "only" $500 or less. These are often the result of massive, spam-type attacks seeking quantity over quality. However, almost 20 percent of ransomware victims have seen demands exceed $10,000, which often are the result of more targeted attacks.

Figure 17
Amounts Demanded by Ransomware Perpetrators



Source: Osterman Research, Inc.

Interestingly, low level ransomware demands (those demanding ransom of up to $500) are most common in the United States and much less common in the other nations surveyed, where between four percent and 19 percent of ransom demands are this low. By contrast, more expensive ransomware demands are more common outside of the United States. For example, ransom demands in excess of $10,000 are most common in Germany (48 percent), but much less common in the United Kingdom (22 percent), the United States (18 percent) and Canada (14 percent).

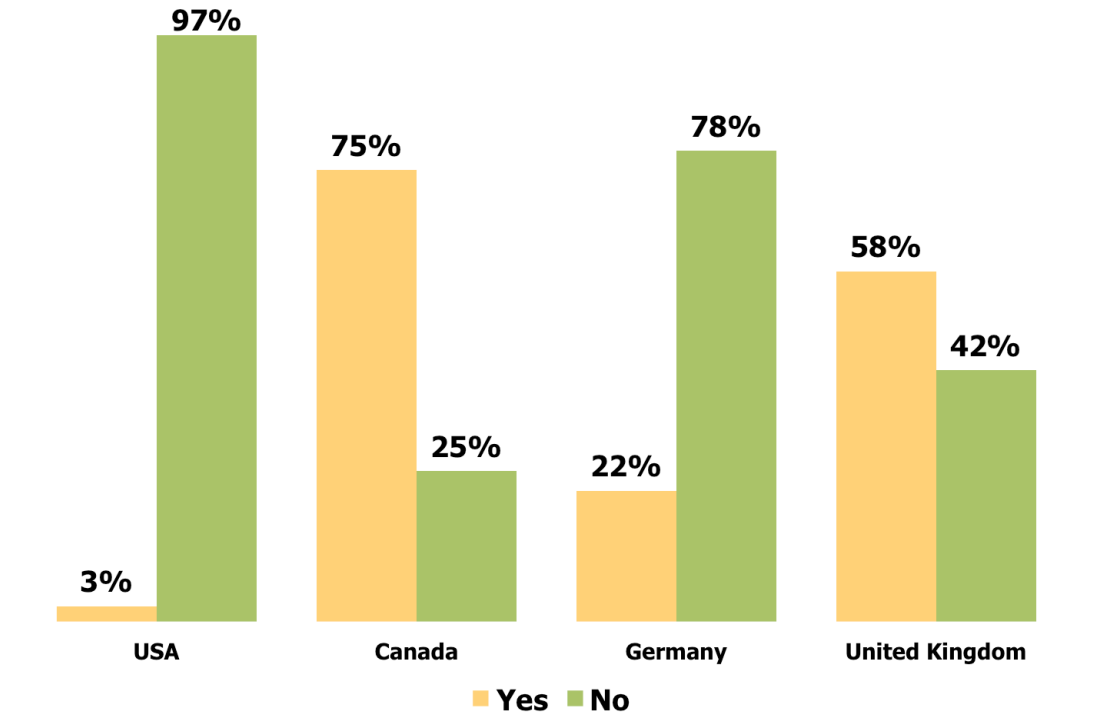
[3] http://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

We attribute much of the "low cost" ransomware activity in the United States to the widespread and growing penetration of ransomware-as-a-service and its use by low-level criminals who are seeking to make quick money. More sophisticated and more expensive ransomware, such as the attack on the Hollywood Presbyterian Medical Center in February 2016 that cost the organization $17,000 in Bitcoin, are less common.

MOST VICTIMS DO NOT PAY THE RANSOM

The majority of ransomware victims surveyed have chosen not to pay the ransom demanded by the cyber criminals that infected their machines, as shown in Figure 18. On average, 37 percent of organizations pay the ransom demanded after they are infected.

Figure 18
Was the Ransomware Paid?



Source: Osterman Research, Inc.

Organizations in the United States were far less likely to pay the ransom demanded once their endpoints are infected with ransomware. For example, 22 percent of German organizations paid the ransom, as did 58 percent of organizations in the United Kingdom and 75 percent of Canadian organizations. Osterman Research believes that the key factor in the dramatically lower level of payment among U.S. organizations is attributable to two factors:

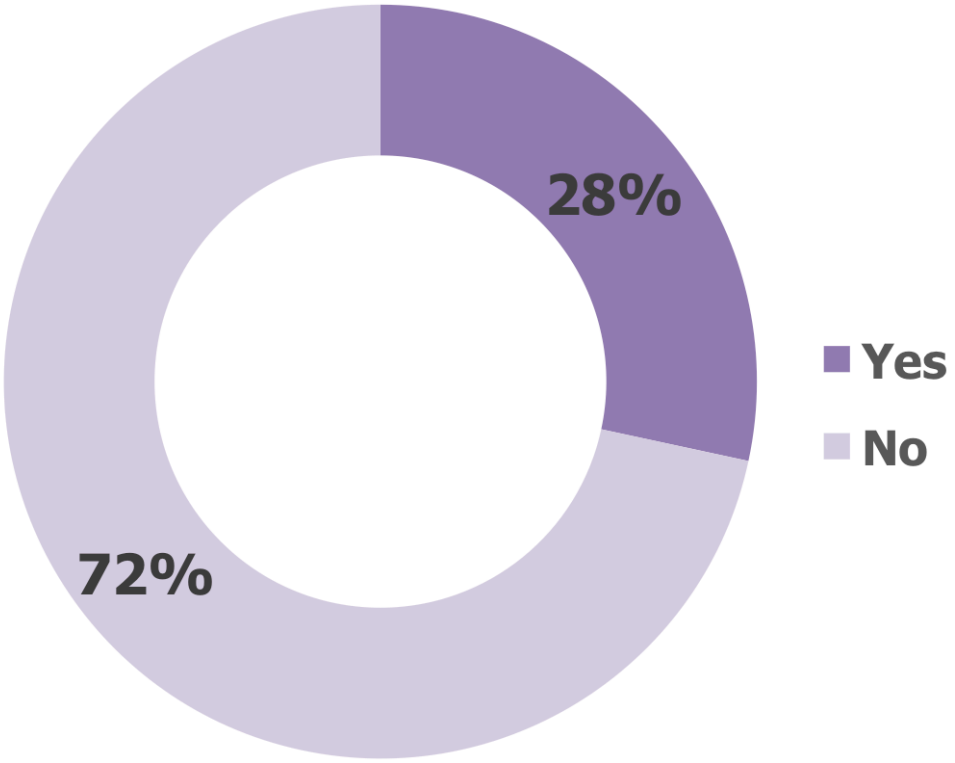
- The much more limited spread of ransomware infections as shown in Figures 13 and 14.
- The fact that lower level employees are more impacted by ransomware than are their counterparts in middle and upper management.

However, the proportion of U.S. organizations that pay the ransom demanded after infection may increase in the future if cyber criminals become more successful in penetrating the C-suite with their wares. In short, the more that senior management is impacted by ransomware, we believe the more likely the organization will be to pay up.

NOT PAYING HAS ITS CONSEQUENCES

Among organizations that chose not to pay the ransom after becoming infected with ransomware, more than one-quarter lost files because they did not pay, as shown in Figure 19.

Figure 19
Did Organizations Lose Files by Not Paying?



Source: Osterman Research, Inc.

The fact that files were lost after a decision not to pay a cyber criminal's ransom demands is not surprising. Because there is rarely a way to decrypt files without the key provided by the ransomware author, the likelihood of being able to thwart the ransomware encryption is nil. Moreover, while most organizations back up their endpoints, these backups are typically performed overnight, and so data created since the last backup can be lost if an endpoint needs to be reimaged in the wake of a ransomware exploit. In short, organizations that choose not to pay ransomware can count on losing at least some files as a result.

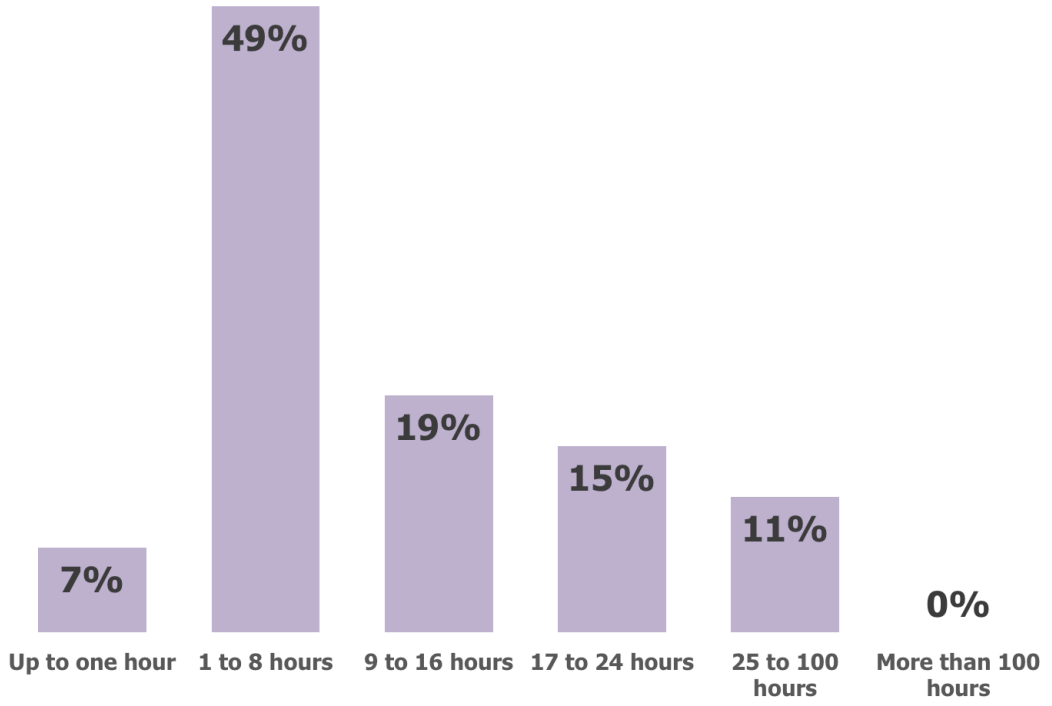
Interestingly, in the other nations surveyed our research found the highest rate of file loss in Canada (82 percent), followed by the United Kingdom (32 percent) and Germany (11 percent).

I.T. DOES NOT SPEND LOTS OF TIME REMEDIATING RANSOMWARE

While 56 percent of ransomware attacks took up to eight hours to remediate, 44 percent of attacks on U.S. companies forced IT staff to work more than nine hours to remediate the incident – the global figure is 63 percent that spend more than nine hours. Further, more than 10 percent of attacks took 25 to more than 100 IT staff hours to remediate.

Most of the organizations infected with ransomware do not spend an inordinate amount of IT staff time recovering from a ransomware attack, as shown in Figure 20. In fact, the majority of organizations spend no more than eight IT staff hours dealing with the aftermath of a ransomware infection, while only a relative small proportion spend significantly more than that.

Figure 20
IT Staff Hours Spent on Remediation



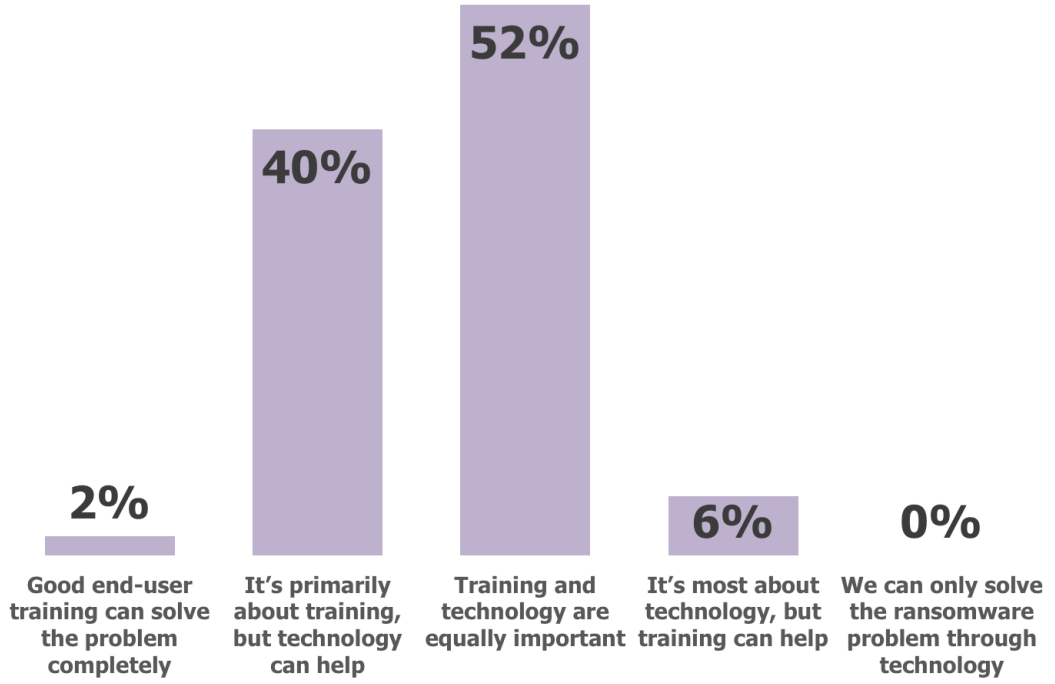
Source: Osterman Research, Inc.

U.S. organizations that must recover from ransomware attacks generally spend less IT staff time doing so than their Canadian, German or UK counterparts. For example, while 56 percent of U.S. organizations spend no more than eight hours recovering from a significant ransomware attack, these figures range from only 20 percent to 30 percent in the other nations surveyed. Osterman Research believes that much of this difference is attributable to the fact that ransomware infiltrations in U.S. organizations spread to fewer endpoints than they do in the other nations surveyed.

TRAINING VS. TECHNOLOGY

Defeating ransomware is a balance between training to help users understand how to reduce their likelihood of becoming infected and technology-based solutions that can help detect ransomware exploits and prevent the infection of endpoints. As shown in Figure 22, U.S. organizations view ransomware prevention and remediation as focused on both training and technology, but lean more toward the former.

Figure 22
Preferred Balance Between Training and Technology to Address the Ransomware Problem



Source: Osterman Research, Inc.

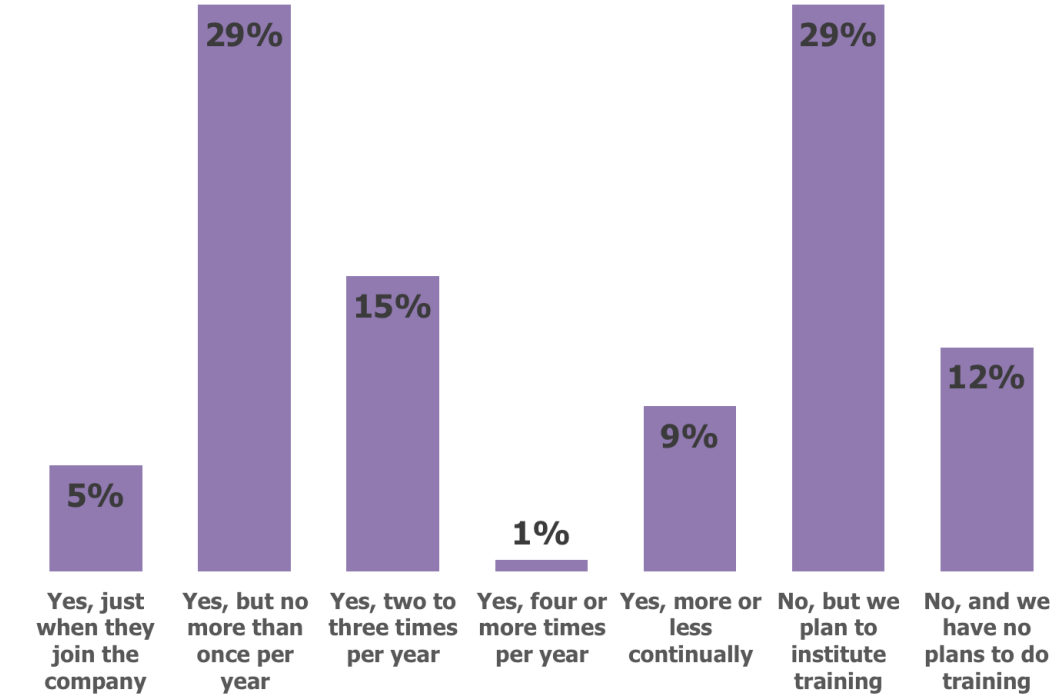
While U.S. organizations tend to lean a bit more toward training as a way to address the ransomware problem, organizations in the other nations we surveyed take a somewhat more technology-centric focus. For example, while only six percent of U.S. organizations believe that dealing with ransomware is mostly a technology problem, this figure is much higher in Germany (22 percent), Canada (27 percent) and the United Kingdom (35 percent).

While there may be several explanations for this fairly significant difference between the U.S. and the other nations surveyed, we go back to the fact that ransomware infiltrations are relatively limited in their tendency to spread to a large number of endpoints. Consequently, some IT decision makers may believe that since only one or a small number of endpoints normally become infected as the result of a typical ransomware attack, educating individual users about good anti-ransomware practices is more appropriate than deploying technology-based solutions.

U.S. ORGANIZATIONS ARE LESS LIKELY TO TRAIN USERS

Roughly three in five organizations provides training to their end users about ransomware, as shown in Figure 23. However, 41 percent of organizations do not currently offer any sort of ransomware education for their end users, but most plan to do so.

Figure 23
Current Level of Training Provided to Employees About Ransomware



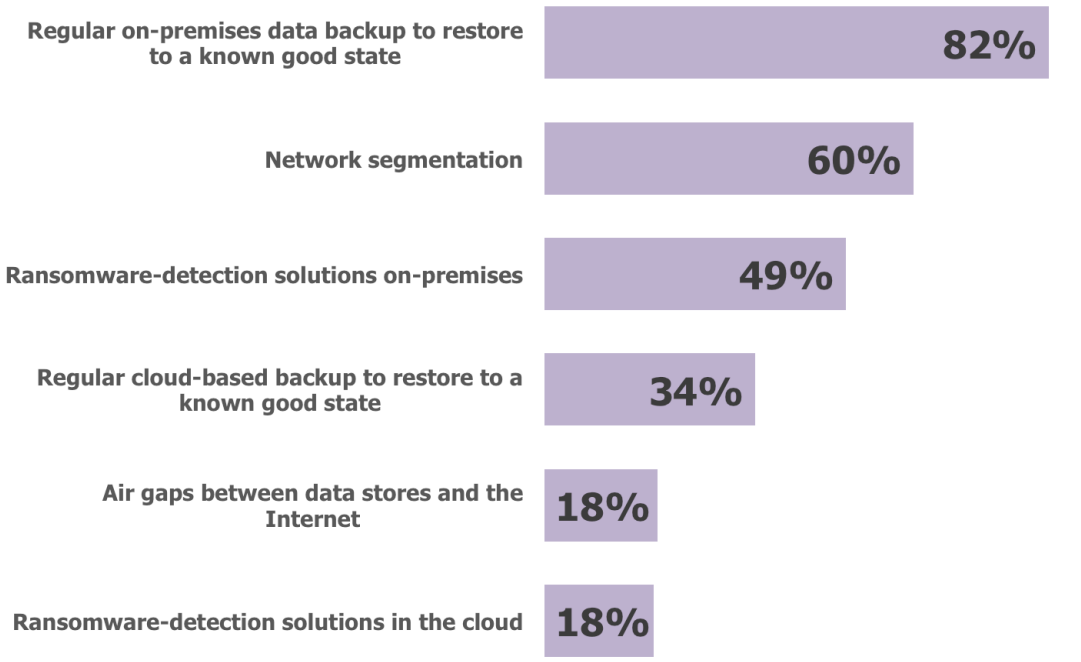
Source: Osterman Research, Inc.

The focus on training vs. technology among U.S. organizations is an interesting one. On the one hand, U.S. organizations slightly tend to favor education as a means of dealing with ransomware as compared to organizations in the other nations surveyed. Somewhat ironically, however, U.S. organizations are also the least likely to have implemented any sort of ransomware training for their end users, and are among the most likely to offer only minimal training.

BACKUP IS THE RECOVERY MODE OF CHOICE FOR MANY

One of the more effective methods for recovering from a ransomware infection is restoring endpoints from backups that occurred prior to the infection. These backups, which allow endpoints to be restored to a known good state from before the infection occurred, are available in more than four out of five of the organizations surveyed, as shown in Figure 24. Other tools in place to address ransomware include network segmentation, employed in three out of five organizations; and on-premises ransomware-detection solutions, deployed in roughly one-half.

Figure 24
Tools in Place to Address Ransomware



Source: Osterman Research, Inc.

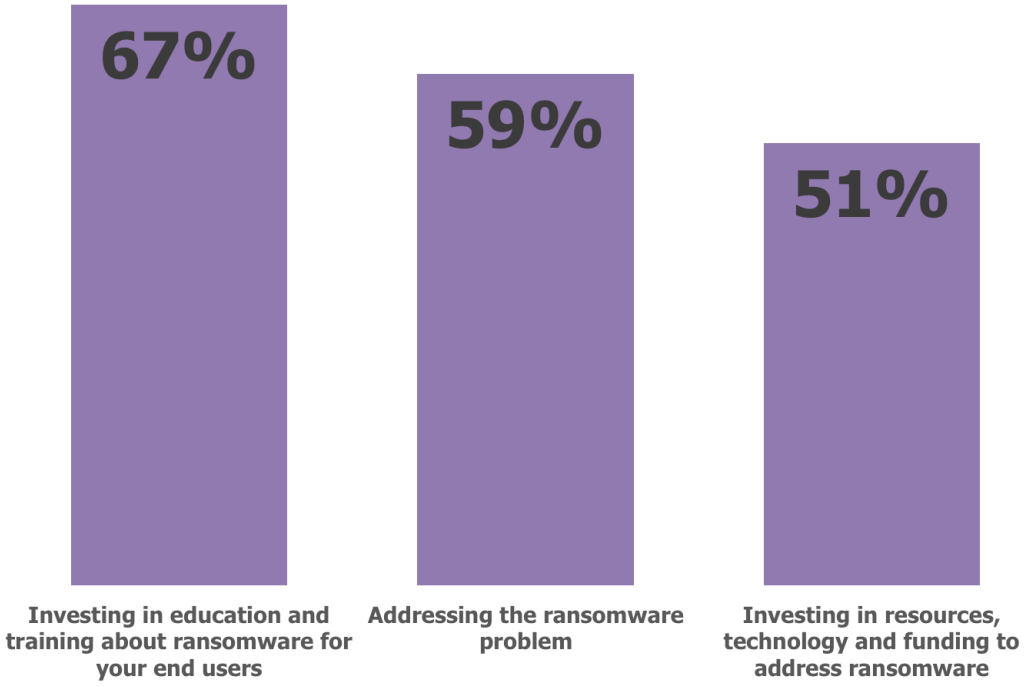
Using backups that will help restore endpoints to a known good state is a common tool employed to remediate ransomware attacks in all of the nations we surveyed, although most common in the United States and Germany. Air gaps among U.S. organizations are used much less often than in the other nations, but on-premises ransomware-detection solutions are much more common in the United States.

The perceived importance of backups as a ransomware-recovery tool is quite high among U.S.-based organizations. In a follow-up survey that Osterman Research completed with a subset of the organizations we originally surveyed (those that chose not to pay the ransom that was demanded from them), the availability of recent backups was cited frequently as the reason that the organization could opt for the decision not to pay the ransom. Although Osterman Research believes that ransomware-detection technologies will be much more widely used in the future than they are today, we anticipate that most decision makers will continue to rely on backups as a ransomware-recovery method indefinitely.

U.S. ORGANIZATIONS WANT TO SOLVE THE RANSOMWARE PROBLEM

U.S. organizations are quite serious about addressing ransomware issues. As shown in Figure 25, two-thirds of the organizations surveyed give a high or very high priority to investing in education and training about ransomware for their end users, while slightly more than one-half give this level of priority to investing in resources, technology and funding to address ransomware. Moreover, almost three in five organizations have established "addressing the ransomware problem" as a high or very priority.

Figure 25
Priority for Addressing Ransomware Issues
% Indicating a High Priority or Very High Priority



Source: Osterman Research, Inc.

U.S. organizations are significantly more concerned about addressing ransomware issues than are their counterparts in the other nations in which we surveyed. For example, the general "addressing the ransomware problem" issue is a high or very high priority for 59 percent of U.S. organizations, but somewhat less in the United Kingdom and Canada (55 percent and 52 percent, respectively), but only 19 percent in Germany.

Moreover, the difference between U.S. organizations and those in the other nations in the survey is even more pronounced when it comes to making investments in anti-ransomware technology and in user education about ransomware issues. This is particularly true for the latter, where 67 percent of U.S. organizations consider user education about ransomware a high or very high priority compared to 35 percent in the United Kingdom, 23 percent in Canada and only nine percent in Germany.

ABOUT MALWAREBYTES

Malwarebytes protects consumers and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware, the company's flagship product, has a highly advanced heuristic detection engine that removed more than five billion malicious threats from computers worldwide. More than 10,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the company is headquartered in California with offices in Europe, and a global team of researchers and experts. For more information, please visit us at www.malwarebytes.com.