Understanding the Depth of the Global Ransomware Problem

An Osterman Research Survey Report

Published August 2016

Sponsored by

Malwarebytes
EXECUTIVE SUMMARY - GLOBAL

This report presents the results of a survey undertaken in the United States, Canada, Germany and the United Kingdom on ransomware and related issues. 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 included in the online survey. Results from the other surveys are available in separate survey reports to be published by Osterman Research and Malwarebytes. The industries surveyed are shown below.

Figure 1
Distribution of Global Industries Surveyed

<table>
<thead>
<tr>
<th>Industry</th>
<th>%</th>
<th>Industry</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services/banking/insurance</td>
<td>20</td>
<td>Education</td>
<td>5</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>12</td>
<td>Telecommunications/ISP</td>
<td>4</td>
</tr>
<tr>
<td>Government</td>
<td>9</td>
<td>Energy/utilities</td>
<td>3</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9</td>
<td>Food/agriculture</td>
<td>2</td>
</tr>
<tr>
<td>Engineering/construction</td>
<td>7</td>
<td>Hospitality</td>
<td>1</td>
</tr>
<tr>
<td>High tech</td>
<td>6</td>
<td>Pharmaceutical</td>
<td>1</td>
</tr>
<tr>
<td>Transportation</td>
<td>6</td>
<td>Law enforcement</td>
<td>1</td>
</tr>
<tr>
<td>Retail/eCommerce</td>
<td>6</td>
<td>Other</td>
<td>11</td>
</tr>
</tbody>
</table>

KEY TAKEAWAYS

- Thirty-nine percent of the organizations we surveyed had been impacted by a ransomware attack during the previous 12 months. Across the various industries surveyed, ransomware attacks were most common in the healthcare industry and in financial services-related industries, including banking and insurance. Among the nations we surveyed, ransomware attacks were most common in the United Kingdom (impacting 54 percent of organizations) and least common in Germany (impacting 18 percent).

  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.

- With regard to the broader category of “security attacks” – e.g., malware infiltrations, denial-of-service attacks, hacking attempts and the like – U.S. companies were the most likely victims, with 79 percent of organizations experiencing some form of security-related breach during the previous 12 months. German companies were the least likely to be attacked, but 65 percent of German companies still suffered some form of security attack during the previous year.

- We found significant variability in terms of decision makers’ confidence with regard to stopping ransomware. For example, 67 percent of Canadian decision makers were either “fairly” or “very” confident about their ability to stop ransomware, while nearly as many German decision makers were this confident. Organizations in the United Kingdom were less confident about their ability to thwart ransomware (58 percent), while U.S. companies were the most pessimistic at only 37 percent indicating this level of confidence.

- Decision makers’ concerns about security-related problems varied widely. In the U.S., for example, the most commonly cited issues about which decision makers are “concerned” or “extremely concerned” are phishing through email (67 percent), malware infiltration through web browsing and malware infiltration through email (both tied at 65 percent), and ransomware (54 percent). Overall, U.S. companies are generally more concerned about the variety of security-
related issues on which we queried survey respondents. 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.

- U.S. organizations are the most likely to make “addressing the ransomware issue” a high or very high priority at 59 percent, while German organizations give this issue the lowest priority (19 percent). U.S. organizations are also more likely to place a high or very high priority on investing in education and training about ransomware for their end users; and for investing in resources, technology, and funding to address the ransomware problem. 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 when they actually do so.

- From a physical platform perspective, ransomware is most likely to enter an organization through a desktop computer and least likely through a smartphone or tablet. German organizations, in particular, had the highest penetration of ransomware infection through desktop computers, while organizations in the U.S. and the United Kingdom had the lowest penetration through desktops.

- Email was the most likely attack vector for ransomware, either via email attachments or malicious links in email messages. Interestingly, a large proportion of the organizations surveyed did not know how the ransomware they encountered had entered — this ranged from a low of nine percent of U.S. organizations that could not identify the source of the ransomware infiltration to a high of 35 percent in Germany.

- Organizations in the U.S. experienced the lowest rate of ransomware infiltration after the initial attack occurred — 58 percent of organizations in the U.S. were able to limit the spread to fewer than one percent of the endpoints. At the other end of the spectrum, 10 percent of the organizations we surveyed in the United Kingdom experienced ransomware spreading to every endpoint on the network.

- A wide variety of corporate roles were impacted by ransomware attacks and this varied widely within the nations we surveyed. For example, ransomware impacted 71 percent of lower level staff members in U.S. organizations, 43 percent of middle managers, and 25 percent of C-level or senior executives. The impact on various roles in other nations was less severe, but generally followed the same pattern.

   It is important to note, however, that 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.

- Ransomware demands from cybercriminals who successfully infiltrated corporate networks varied widely. In the U.S., 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. Interestingly, low level ransomware demands (those demanding ransom of up to $500) are most common in the U.S. 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 U.S. 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)

1 Please note that we converted U.S. currencies to the appropriate non-U.S. currency when conducting the survey so that respondents could answer these questions in their national currency. Currency conversion rates were those in effect as of mid-June 2016.
• The majority of ransomware victims surveyed have chosen not to pay the ransom demanded by the cybercriminals that infected their machines. On average, 37 percent of organizations pay the ransom demanded after they are infected. 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, but only three percent of U.S. organizations chose to do so.

• Among organizations that chose not to pay the ransom after becoming infected with ransomware, more than one-quarter of U.S. organizations lost files because they did not pay. However, this varied widely by nation surveyed: 82 percent of Canadian organizations that opted not to pay ransom lost files as a result, whereas this decision impacted "only" 11 percent of German organizations.

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 of their files as a result.

• 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.

• 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. 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).

• The perceived importance of regular, on-premises backups as a ransomware-recovery tool is quite high among U.S. and German organizations, but somewhat lower among the organizations we surveyed in Canada and the United Kingdom. However, Canadian and UK-based organizations were more likely to use regular, cloud-based backups to recover from ransomware. Other capabilities in place to address ransomware included on-premises ransomware-detection solutions (highest penetration in the U.S.), network segmentation (highest in Germany), and air gaps between data stores and the Internet (highest in Canada).

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.
EXECUTIVE SUMMARY – UNITED STATES

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 included in the online survey. Results from the other surveys are available in separate survey reports. The distribution of industries surveyed in the U.S. is shown in Figure 2.

Figure 2
Distribution of US Industries Surveyed

<table>
<thead>
<tr>
<th>Industry</th>
<th>%</th>
<th>Industry</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>18</td>
<td>Retail/eCommerce</td>
<td>4</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>14</td>
<td>Engineering/construction</td>
<td>3</td>
</tr>
<tr>
<td>Financial services/banking/insurance</td>
<td>13</td>
<td>Energy/utilities</td>
<td>2</td>
</tr>
<tr>
<td>High tech</td>
<td>10</td>
<td>Food/agriculture</td>
<td>2</td>
</tr>
<tr>
<td>Education</td>
<td>8</td>
<td>Hospitality</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>8</td>
<td>Law enforcement</td>
<td>1</td>
</tr>
<tr>
<td>Telecommunications/ISP</td>
<td>4</td>
<td>Pharmaceutical</td>
<td>1</td>
</tr>
<tr>
<td>Transportation</td>
<td>4</td>
<td>Other</td>
<td>8</td>
</tr>
</tbody>
</table>
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 3. More than one-quarter of those attacked have experienced more than 20 security attacks during the past year.

Figure 3
Security Attacks During the Previous 12 Months

![Figure 3 Graph](image)

Source: Osterman Research, Inc.

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

U.S. organizations are the most attacked among the organizations that we surveyed. For example, as shown in Figure 4, 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 4
Security Attacks That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>21%</td>
<td>28%</td>
<td>35%</td>
<td>28%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>13%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>10%</td>
<td>20%</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>5%</td>
<td>30%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>More than 20</td>
<td>22%</td>
<td>9%</td>
<td>10%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
NEARLY ONE-HALF HAVE EXPERIENCED RANSOMWARE ATTACKS
As shown in Figure 5, 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 5
Ransomware Attacks During the Previous 12 Months

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 6. 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 6
Ransomware Attacks That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>53%</td>
<td>65%</td>
<td>82%</td>
<td>46%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>27%</td>
<td>18%</td>
<td>42%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>4%</td>
<td>7%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>More than 20</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
</tbody>
</table>

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 7. Twelve percent of companies in the U.S. had to stop business immediately upon discovering the ransomware attack.

Figure 7
Values of the Files That Were Encrypted

| People were personally impacted (customers, students, vendors, staff, etc.) | 78% |
| It stopped business immediately | 12% |
| Employees used personally owned smartphones, tablets or laptops because corporate systems were down | 11% |
| We lost revenue | 6% |
| Lives were at stake | 0% |

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 8, 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 8
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 9. 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 9
Confidence in the Ability to Stop Ransomware

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 10, 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.

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 11.

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 12. Mobile devices and servers are not common entry points for ransomware, but one in 14 organizations is not sure of the source.
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, 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. 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 13. 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 they don’t know the applications by which ransomware entered the organization.

![Figure 13](http://www.ostermanresearch.com/images/f13.jpg)

**Applications by Which Ransomware Entered the Organization**

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email link</td>
<td>31%</td>
</tr>
<tr>
<td>Email attachment</td>
<td>28%</td>
</tr>
<tr>
<td>A Web site or Web application other than email or social media</td>
<td>24%</td>
</tr>
<tr>
<td>Social media</td>
<td>4%</td>
</tr>
<tr>
<td>USB stick</td>
<td>3%</td>
</tr>
<tr>
<td>Business application</td>
<td>1%</td>
</tr>
<tr>
<td>We don’t know</td>
<td>9%</td>
</tr>
</tbody>
</table>

*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

---

2 http://www.statisticbrain.com/computer-sales-statistics/
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 14 and 15, 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 14**

Proportion of Endpoints to Which Ransomware Attacks Spread

![Bar Chart]

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.
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 17.

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.4"

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 18, 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.

![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).

---

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 19. On average, 37 percent of organizations pay the ransom demanded after they are infected.

![Figure 19: Was the Ransomware Paid?](image)

Source: Osterman Research, Inc.

Organizations in the United States were far less likely to pay the ransom demanded once their endpoints were 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.
- 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 20.

![Diagram showing file loss after not paying ransom](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 21. 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 21**

IT Staff Hours Spent on Remediation

<table>
<thead>
<tr>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to one hour</td>
<td>7%</td>
</tr>
<tr>
<td>1 to 8 hours</td>
<td>49%</td>
</tr>
<tr>
<td>9 to 16 hours</td>
<td>19%</td>
</tr>
<tr>
<td>17 to 24 hours</td>
<td>15%</td>
</tr>
<tr>
<td>25 to 100 hours</td>
<td>11%</td>
</tr>
<tr>
<td>More than 100 hours</td>
<td>0%</td>
</tr>
</tbody>
</table>

*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.
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.
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.
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.
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.
EXECUTIVE SUMMARY - CANADA

KEY TAKEAWAYS

- Seventy-two percent of Canadian organisations have been the victim of a cyber attack during the past 12 months. Thirty-five percent have been the victim of a ransomware attack.

- Ransomware attacks among Canadian organisations have had a reasonably significant impact: nearly two-thirds of successful ransomware attacks are able to reach up to 25 percent of endpoints, and one-third more have impacted up to 50 percent of endpoints.

- Canadian survey results show that 22 percent of attacks impacted mid-level managers or higher, with eight percent of incidents attacking senior executives and the C-Suite.

- The business impact in Canada was high, with 43 percent of the organisations surveyed reporting lost revenue and 25 percent revealing a stop in business operations as a result of a ransomware infection. Eleven percent claimed that lives were at risk from ransomware, the highest percentage among the regions surveyed.

- Canadian organisations were the most likely to pay ransom demands (75 percent) and if they didn't pay, 82 percent lost files. Globally, nearly 40 percent of ransomware victims paid the ransom.

- The cost of ransomware attacks in Canada is much higher than in the U.S., with the majority of attacks costing between $1,000 and $50,000.

- The most heavily targeted industries for ransomware are healthcare and financial services.

ABOUT THIS SURVEY REPORT

This report presents the US 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 Canadian organisations. The survey was conducted during June 2016 with 165 organisations 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 organisation. A total of 21 questions were included in the online survey. Results from the other surveys are available in separate survey reports. The distribution of industries surveyed in Canada is shown in Figure 26.

Figure 26
Distribution of Canadian Industries Surveyed

<table>
<thead>
<tr>
<th>Industry</th>
<th>%</th>
<th>Industry</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>18%</td>
<td>Education</td>
<td>4%</td>
</tr>
<tr>
<td>Transportation</td>
<td>14%</td>
<td>Telecommunications/ISP</td>
<td>4%</td>
</tr>
<tr>
<td>Engineering/construction</td>
<td>14%</td>
<td>Energy/utilities</td>
<td>3%</td>
</tr>
<tr>
<td>Financial services/banking/insurance</td>
<td>11%</td>
<td>Government</td>
<td>2%</td>
</tr>
<tr>
<td>High tech</td>
<td>9%</td>
<td>Food/agriculture</td>
<td>2%</td>
</tr>
<tr>
<td>Retail/eCommerce</td>
<td>6%</td>
<td>Hospitality</td>
<td>1%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5%</td>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>
SURVEY FINDINGS

During the previous 12 months, nearly more than 70 percent of Canadian organisations have experienced some kind of security attack, as shown in Figure 27. However, nearly 10 percent have experienced more than 20 security attacks during the last 12 months.

Figure 27
Security Attacks During the Previous 12 Months

Source: Osterman Research, Inc.

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

Figure 28
Attacks That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>21%</td>
<td>28%</td>
<td>35%</td>
<td>28%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>13%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>10%</td>
<td>20%</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>5%</td>
<td>30%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>More than 20</td>
<td>22%</td>
<td>9%</td>
<td>10%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
MORE THAN A THIRD HAVE BEEN IMPACTED BY RANSOMWARE

In the past year, “only” 35 percent of Canadian organisations surveyed have experienced a ransomware attack, as shown in Figure 29. Out of those that have experienced a ransomware attack, the majority have encountered anywhere from one to five infections during the past year.

Figure 29
Ransomware Attacks During the Previous 12 Months

Our research found that Canadian and German organisations experience significantly fewer ransomware attacks relative to U.S. organisations, but that those in the United Kingdom experience ransomware attacks to a slightly greater degree – 54 percent of organisations in the United Kingdom have experienced ransomware attacks compared to 47 percent in the United States, as shown in Figure 30. 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.
Ransomware Infections Can Be Widespread

While some Canadian organisations impacted by ransomware have seen fewer than one percent of endpoints impacted by serious ransomware attacks, the vast majority have seen attacks spread to up to 50 percent of their endpoints, as seen in Figure 31 and 32.

While more organisations in the United Kingdom saw the spread of ransomware to 100 percent of the endpoints once they were infected, Canadian organisations were also heavily impacted by ransomware: more than two in five Canadian organisations reported that malware infections impacted more than 25 percent of the endpoints on the network.
The impact of ransomware on Canadian organisations is significant relative to the other nations surveyed in a couple of ways. First, ransomware victims in Canada were much less able to contain the spread of the infection to fewer than one percent of the endpoints when compared to organisations in the United States. Second, Canada is the only other nation surveyed beside the United Kingdom in which some ransomware infections spread to the entire corporate network.

**LOW-LEVEL STAFF ARE EASY TARGETS, C-LEVEL EXECUTIVE ALSO AT RISK**

The majority of Canadian organisations 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, and mid-level managers, as shown in Figures 33 and 34. However, senior corporate executives are also victims.
Figure 33
Roles Impacted by Ransomware Attacks

<table>
<thead>
<tr>
<th>Role</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower level staff members/clerical staff</td>
<td>71%</td>
<td>23%</td>
<td>14%</td>
<td>29%</td>
</tr>
<tr>
<td>Mid-level managers</td>
<td>43%</td>
<td>22%</td>
<td>13%</td>
<td>42%</td>
</tr>
<tr>
<td>C-level or other senior executives</td>
<td>25%</td>
<td>8%</td>
<td>6%</td>
<td>15%</td>
</tr>
<tr>
<td>External staff (e.g., consultants, contractors, vendors etc.)</td>
<td>9%</td>
<td>2%</td>
<td>2%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

Figure 34
Roles That Have Been Impacted by Ransomware

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. 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 kidde’ who deployed the attack.5

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.

SOME MAJOR IMPACTS FROM RANSOMWARE ON CANADIAN ORGANISATIONS
The impact of ransomware was significant among organisations that were infected, primarily in the context of its impact personal productivity, files lost, etc. as shown in Figure 35. However, many organisations lost revenue and had their business immediately stopped. In 11 percent of cases, lives were at stake.

Figure 35
Values of the Files That Were Encrypted

<table>
<thead>
<tr>
<th>Impact Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>People were personally impacted (customers, students, vendors, staff, etc.)</td>
<td>66%</td>
</tr>
<tr>
<td>We lost revenue</td>
<td>43%</td>
</tr>
<tr>
<td>It stopped business immediately</td>
<td>25%</td>
</tr>
<tr>
<td>Employees used personally owned smartphones, tablets or laptops because corporate systems were down</td>
<td>16%</td>
</tr>
<tr>
<td>Lives were at stake</td>
<td>11%</td>
</tr>
</tbody>
</table>

<Source: Osterman Research, Inc.>

Canadian organisations were the second most likely among the nations we surveyed to report loss of revenue from a malware infection, and they were the most likely to have their operation cease immediately upon the infection taking hold.

MOST RANSOMWARE VICTIMS PAY UP
Three-quarters of Canadian ransomware victims have chosen to pay the ransom demanded by the cyber criminals, as shown in Figures 36 and 37. Only 25 percent have decided not to pay the ransom. Among the nations we surveyed, organisations in Canada were significantly more likely to pay ransom demands than organisations in other countries.

Figure 36
Was the Ransomware Paid?

Source: Osterman Research, Inc.

Figure 37
Was the Ransomware Paid?

Source: Osterman Research, Inc.
MOST NON-PAYERS LOSE FILES
As shown in Figure 38, among the organisations that chose not to pay after being infected with ransomware, the vast majority lost files because they did not pay; only 18 percent were unaffected by their decision not to pay.

Interestingly and somewhat ironically, Canadian organisations were the most likely to pay ransomware demands AND the most likely to lose files if they chose not to pay. The fact that files were lost after a decision not to pay a cyber criminal’s ransom demands is not surprising, but the relative proportion in Canada that lost files is a bit perplexing. 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 organisations 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, organisations that choose not to pay ransomware can count on losing at least some files as a result.

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).

RANSOMWARE DEMANDS ARE SIGNIFICANT
As shown in Figure 39, the most common amounts demanded by ransomware perpetrators is no more than CDN$6,500. Those who faced demands of “only” CDN$650 or less constituted around nine percent of organisations surveyed, while 30 percent of organisations have seen demands upwards of CDN$13,000.
Interestingly, low level ransomware demands (those demanding ransom of up to US$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 US$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). Although ransomware in Germany may be less common than it is in other nations, it is significantly more expensive when it does occur.

**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 40, 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.
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 organisations 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 organisations in these industries, particularly for highly targeted, spearphishing-like attacks.
DESKTOP COMPUTERS ARE A COMMON INGRESS POINT
Among organisations that have experienced a ransomware attack, roughly three in five have encountered the attack through a desktop computer. As shown in Figure 41, servers and mobile devices were the least common entry points for ransomware, but 16 percent still do not know where the ransomware entered their organisation.

Figure 41
Physical Locations in Which Ransomware Entered the Organisation

![Figure 41](image)

Source: Osterman Research, Inc.

Interestingly, Canadian organisations were the most likely among those we surveyed to find that ransomware had entered their organisation through a smartphone or tablet. German organisations reported the highest level of ransomware infection via desktop computers among the nations we surveyed, as well as the highest level of infection through servers. Moreover, organisations in Germany reported much lower ransomware ingress through laptops or mobile devices. By contrast, U.S. organisations reported the lowest level of malware infiltration from desktop computers (49 percent in the US compared to 49 percent to 74 percent in the other nations surveyed), but the highest level of infiltration from laptops (36 percent in the US versus 0 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, 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. That said, unknown

---

6 http://www.statisticbrain.com/computer-sales-statistics/
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).

**BUSINESS APPLICATIONS ARE AN INGRESS POINT**

Business applications lead the way by which ransomware enters organisations in Canada, with 18 percent of organisations finding that they were infected by ransomware through such an application, as shown in Figure 42. Other common entry points are email attachments, web site or web applications and email links. However, one-quarter of those surveyed do not know the applications by which ransomware entered the organisations. Unknown sources of ransomware were much higher than in the U.S., but significantly lower than in either Germany or the United Kingdom.

---

**Figure 42**

*Applications by Which Ransomware Entered the Organisation*

- **Business application**: 18%
- **Email attachment**: 16%
- **A Web site or Web application other than email or social media**: 16%
- **Email link**: 14%
- **USB stick**: 7%
- **Social media**: 5%
- **We don't know**: 25%

*Source: Osterman Research, Inc.*
FALSE SENSE OF SECURITY ABOUT STOPPING RANSOMWARE

With the highest penetration rate and highest business impact with respect to disruption, Canadian’s have a false sense of security with 51 percent fairly confident in their ability to stop ransomware. Among organisations surveyed in Canada, more than two-thirds are fairly confident or very confident in their ability to stop ransomware, as shown in Figure 43. However, roughly one-third of Canadian organisations have relatively little confidence in their ability to stop ransomware.

Figure 43
Confidence in the Ability to Stop Ransomware

Our research showed that across the organisations in the four nations surveyed, Canadian organisations had the highest level of confidence in their ability to stop ransomware: 67 percent are either "fairly" or "very" confident in their ability, followed by organisations in Germany (66 percent), the United Kingdom (58 percent), and the United States (37 percent). The high level of confidence in both Canada and Germany may be partially the result of relatively low ransomware penetration in both countries relative to the others.
RANSOMWARE IS A SIGNIFICANT CONCERN

Ransomware is a concern or extreme concern for about one-third of Canadian organisations, as shown in Figure 44. While ransomware does not rank as highly as a concern among Canadian organisations as it does among their counterparts in the U.S. or the United Kingdom, it is still a major concern even in the context of the other security issues about which respondents were queried. The variety of security-related concerns across the four nations surveyed is shown in Figure 45.

Figure 44
Concerns About Security-Related Problems
Percent Responding Concerned or Extremely Concerned

<table>
<thead>
<tr>
<th>Security-Related Problems</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infiltration through email</td>
<td>67%</td>
<td>29%</td>
<td>26%</td>
<td>43%</td>
</tr>
<tr>
<td>Malware infiltration via web browsing</td>
<td>65%</td>
<td>33%</td>
<td>23%</td>
<td>46%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>65%</td>
<td>44%</td>
<td>43%</td>
<td>53%</td>
</tr>
<tr>
<td>Phishing through email</td>
<td>54%</td>
<td>32%</td>
<td>12%</td>
<td>50%</td>
</tr>
<tr>
<td>Phishing through social media</td>
<td>36%</td>
<td>17%</td>
<td>14%</td>
<td>23%</td>
</tr>
<tr>
<td>Insider theft of data</td>
<td>30%</td>
<td>5%</td>
<td>4%</td>
<td>10%</td>
</tr>
<tr>
<td>Physical theft of laptops and mobile devices</td>
<td>30%</td>
<td>10%</td>
<td>5%</td>
<td>34%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
It is important to note, however, that U.S. organisations 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.

**IT SPENDS LOTS OF TIME DEALING WITH THE AFTERMATH OF RANSOMWARE**

Most of the organisations infected with ransomware spend quite a bit of time on remediation. More than three-quarters spent more than nine IT staff hours dealing with the aftermath of a successful ransomware attack, while seven percent of organisations spent more than 100 hours on remediation, as seen in Figure 46. The proportion of Canadian organisations that spent more than 100 hours dealing with ransomware cleanup was the highest among the nations we surveyed.

**Figure 46**

IT Staff Hours Spent on Remediation

Source: Osterman Research, Inc.
CANADIANS TAKE A GENERALLY BALANCED APPROACH IN THEIR ATTEMPTS TO PREVENT RANSOMWARE

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 47, Canadian organisations view ransomware prevention and remediation as focused on both training and technology, but lean slightly towards the latter. Among the nations we surveyed, Canadian organisations take the most balanced approach between training and technology.

Figure 47
Preferred Balance Between Training and Technology to Address the Ransomware Problem

Source: Osterman Research, Inc.
CANADIAN RANSOMWARE TRAINING IS SIMILAR TO THE US PATTERN

As shown in Figure 48, the majority of Canadian organisations provide training to employees about ransomware. Although 23 percent of organisations do not currently offer any sort of ransomware education for their employees, most of these organisations have plans to institute training at some point.

Figure 48
Current Level of Training Provided to Employees About Ransomware

Source: Osterman Research, Inc.
**NETWORK SEGMENTATION IS COMMONLY EMPLOYED TO MITIGATE THE IMPACT OF RANSOMWARE**

Out of the organisations surveyed, seven out of ten choose to use network segmentation as one of their tools to address ransomware. Regular, on-premises data backup is also used by 60 percent of organisations, as shown in Figure 49. Ransomware-detection solutions – both on-premises and in the cloud – are lower priority tools to address the ransomware problem.

![Figure 49: Tools in Place to Address Ransomware](source: Osterman Research, Inc.)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network segmentation</td>
<td>70%</td>
</tr>
<tr>
<td>Regular on-premises data backup to restore to a known good state</td>
<td>60%</td>
</tr>
<tr>
<td>Regular cloud-based backup to restore to a known good state</td>
<td>54%</td>
</tr>
<tr>
<td>Air gaps between data stores and the Internet</td>
<td>49%</td>
</tr>
<tr>
<td>Ransomware-detection solutions on-premises</td>
<td>21%</td>
</tr>
<tr>
<td>Ransomware-detection solutions in the cloud</td>
<td>21%</td>
</tr>
</tbody>
</table>

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 Germany and the United States. Air gaps were more often cited by Canadian organisations than others as an anti-ransomware capability. However, German organisations were the most likely among the nations we surveyed to use regular, on-premise data backups and network segmentation as tools to mitigate the impact of ransomware.
SIGNIFICANT INTEREST IN SOLVING RANSOMWARE

More than one-half of Canadian organisations surveyed place a high or very high priority on addressing the ransomware problem, as shown in Figure 50. However, fewer than one-quarter give high or very high priority to investing in education and training about ransomware for their end users, while 38 percent have established investing in resources, technology, and funding to address ransomware as a high or very high priority.

Figure 50
Priority for Addressing Ransomware Issues
Percent Indicating a High Priority or Very High Priority

Source: Osterman Research, Inc.

U.S. organisations 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. organisations, 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. organisations 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 US organisations 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.
EXECUTIVE SUMMARY – UNITED KINGDOM

KEY TAKEAWAYS

• One-half of corporate decision makers in UK-based organisations consider ransomware to be a “concern” or “extreme concern”, the second highest level of concern we discovered among organisations in the nations we surveyed.

• More than 70 percent of organisations have been the victim of a cyber attack during the past 12 months, and 54 percent have been the victim of a ransomware attack – both are among the highest levels of attack we discovered in our research.

• The most heavily targeted industries for ransomware are healthcare and financial services.

• Decision makers in UK-based organisations have a fairly high level of confidence in their ability to effectively stop ransomware: 21 percent of UK-based organisations are “very confident” in their ability to stop ransomware attacks (the highest level we found in our research) and another 37 percent are “fairly confident”.

• Nearly two-thirds of UK-based organisations breached have had high-value data held for ransom, but these organisations were the most likely to report that revenue was lost as a result of a ransomware attack. Most of the victims of ransomware in UK-based organisations were mid-level managers.

• UK-based organisations are heavily committed to solving the ransomware problem: 55 percent report that addressing the ransomware problem is a high or very high priority, and 50 percent consider investing in resources and technology to address ransomware to be this high a priority.

• Ransomware attacks among UK-based organisations have had a significant impact: in 10 percent of the organisations surveyed, the most serious ransomware attacks penetrated every endpoint on the network. In fact, these organisations had the lowest proportion of small-scale ransomware infections (those that penetrated fewer than one percent of endpoints).

• Globally, nearly 40 percent of ransomware victims paid the ransom.

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 UK-based organisations. The survey was conducted during June 2016 with 165 organisations 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 organisation. A total of 21 questions were included in the online survey. Results from the other surveys are available in separate survey reports. The distribution of industries surveyed in the UK is shown in Figure 51.
SURVEY FINDINGS

During the previous 12 months, 72 percent of UK-based organisations surveyed have suffered a security attack, as shown in Figure 52. The majority of the organisations that were infiltrated have experienced a relatively low number of attacks, but one in 10 organisations have been the victim of more than 20 security attacks during the previous year.

Figure 52
Security Attacks During the Previous 12 Months

![Bar chart showing security attacks during the previous 12 months: 28% None, 22% 1 to 5, 25% 6 to 10, 15% 11 to 20, 10% More than 20.]

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. organisations are the most attacked among the organisations, but UK-based are a close second. For example, as shown in Figure 53, between 28 percent and 35 percent of the organisations in the nations we surveyed reported no security-related attacks during the previous 12 months versus 21 percent for U.S. organisations. At the other end of the scale, 22 percent of U.S. organisations reported that they had received more than 20 attacks during the previous year compared to between 8 percent and 10 percent for organisations in the other nations surveyed.
ORGANISATIONS IN THE UK ARE MOST LIKELY TO RECEIVE RANSOMWARE

As shown in Figure 54, nearly one-half of the UK-based organisations surveyed have not experienced a single ransomware attack during the past 12 months, but these organisations are the most likely to be attacked among those we surveyed. Most of the organisations that have experienced such an attack have gone through no more than five ransomware attacks during the past year.

Our research found that Canadian and German organisations experience significantly fewer ransomware attacks relative to organisations, far fewer than in the United Kingdom or the United States – 54 percent of organisations in the United Kingdom have experienced ransomware attacks compared to 47 percent in the United States, as shown in Figure 55. 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

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>21%</td>
<td>28%</td>
<td>35%</td>
<td>28%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>13%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>10%</td>
<td>20%</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>5%</td>
<td>30%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>More than 20</td>
<td>22%</td>
<td>9%</td>
<td>10%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
higher proportion of financial services and related firms in the United Kingdom sample, which may have skewed the results slightly higher.

Figure 55
Ransomware Attacks That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>53%</td>
<td>65%</td>
<td>82%</td>
<td>46%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>27%</td>
<td>18%</td>
<td>42%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>4%</td>
<td>7%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>More than 20</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

MAJOR IMPACTS FROM RANSOMWARE
As shown in Figure 56, the impact of ransomware for UK-based organisations has been significant: 64 percent of these attacks impacted personal productivity and caused users to lose information. More significantly, however, three in five UK-based organisations lost revenue as the result of a ransomware attack – by far the highest level we discovered in our research.

Figure 56
Values of the Files That Were Encrypted

People were personally impacted (customers, students, vendors, staff, etc.) 64%
We lost revenue 60%
It stopped business immediately 24%
Employees used personally owned smartphones, tablets or laptops because corporate systems were down 21%
Lives were at stake 1%

Source: Osterman Research, Inc.
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 57, 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.

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 organisations 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 organisations in these industries, particularly for highly targeted, spearphishing-like attacks.
STRONG CONFIDENCE IN THE ABILITY TO DEFEAT RANSOMWARE

Nearly three in five of the UK-based organisations we surveyed are either “fairly” or “very” confident in their ability to stop ransomware, as shown in Figure 58.

Organisations in the United Kingdom are much more confident about their ability to stop ransomware than organisations in the United States, despite similar levels of infection. We attribute at least part of the greater confidence among UK-based organisations to the significantly higher levels of ransomware-related training that British users receive: 78 percent of UK-based organisations provide some level of training to their end users compared with only 59 percent in the United States.
RANSOMWARE IS A LEADING AREA OF CONCERN IN THE UK
Ransomware is the second leading area of security concern for UK-based organisations, as shown in Figures 59 and 60. In fact, the UK is the only nation we surveyed in which ransomware was the second highest area of concern – in all of the other nations surveyed, ransomware was less of a concern than the other issues about which we queried.

Figure 59
Concerns About Security-Related Problems
Percent Responding Concerned or Extremely Concerned

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infiltration through email</td>
<td>53%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>50%</td>
</tr>
<tr>
<td>Malware infiltration via web browsing</td>
<td>46%</td>
</tr>
<tr>
<td>Phishing through email</td>
<td>43%</td>
</tr>
<tr>
<td>Insider theft of data</td>
<td>34%</td>
</tr>
<tr>
<td>Phishing through social media</td>
<td>23%</td>
</tr>
<tr>
<td>Physical theft of laptops and mobile devices</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

The high level of concern for ransomware relative to other security-related issues is not a surprise: ransomware has penetrated UK-based organisations heavily and has infected the greatest number of endpoints among the nations we surveyed. We anticipate that ransomware will remain a top-of-mind concern for decision makers in UK-based organisations and will likely become a more important issue for them.
### Figure 60
Concerns About Various Security-Related Threats

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

Source: Osterman Research, Inc.

It is important to note that U.S. organisations 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 ARE A COMMON INGRESS POINT FOR RANSOMWARE**

Similar to what our research discovered in the United States, we found that desktop computers were an entry point for ransomware in nearly one-half of UK-based organisations, as shown in Figure 61. However, UK-based organisations had the highest level of “unknown” sources of ransomware ingress among the organisations we surveyed.

![Physical Locations in Which Ransomware Entered the Organisation](source)

Table: Physical Locations in Which Ransomware Entered the Organisation

<table>
<thead>
<tr>
<th>Source: Osterman Research, Inc.</th>
</tr>
</thead>
</table>

UK-based and U.S.-based organisations reported the lowest level of ransomware infection via desktop computers among the nations we surveyed, but UK-based organisations were twice as likely to be infected via a server. UK-based organisations were much more likely to be infected via a laptop than their German counterparts, but much less likely than organisations in the United States.

Part of the difference between organisations in the United Kingdom and United States 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[^8], 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[^9]. 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).

[^8]: http://www.statisticbrain.com/computer-sales-statistics/
EMAIL IS A KEY WAY FOR RANSOMWARE TO ENTER
As shown in Figure 62, email attachments and links were relatively common ways for ransomware to enter an organisation, but these were significantly less common methods of ingress than in the United States. Three out of 10 UK-based organisations did not know the application by which ransomware entered their organisations.

Figure 62
Applications by Which Ransomware Entered the Organisation

- Email attachment: 24%
- Email link: 15%
- Business application: 15%
- A Web site or Web application other than email or social media: 10%
- USB stick: 4%
- Social media: 1%
- We don’t know: 30%

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 ransomware infiltration in the United Kingdom and Canada than in the other nations in which we surveyed, accounting for only 1.3 percent of infiltrations in the United States.
MANY RANSOMWARE INFECTIONS ARE WIDESPREAD
As shown in Figures 63 and 64, when ransomware infects endpoints in UK-based organisations, the impact can be quite damaging. Only a tiny proportion of UK-based organisations reported that ransomware infections spread to fewer than one percent of endpoints, but about one-half reported more widespread infections. More seriously, however, one in 10 UK-based organisations reported that their most serious ransomware infection had reached every endpoint on their networks.

Figure 63
Proportion of Endpoints to Which Ransomware Attacks Spread

Source: Osterman Research, Inc.
RANSOMWARE HITS MID-LEVEL MANAGERS THE MOST

Our research showed that mid-level managers were the hardest hit by ransomware in UK-based organisations, as shown in Figures 65 and 66. Lower level staff members and C-level executives were less impacted in terms of the sheer numbers of ransomware victims. However, it is essential to keep in mind that while 42 percent of the organisations reported that mid-level managers were impacted by ransomware attacks, these managers represent a relatively small proportion of total employees in the typical organisation, as do C-level executives. Consequently, managers are disproportionately impacted by ransomware relative to lower level employees and, because they often deal with more sensitive and confidential data, are much more attractive targets for cybercriminals.
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. 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 5 percent to 20 percent — and the rest goes to the ‘script kiddie’ who deployed the attack.\textsuperscript{10}

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.

**UK RANSOM DEMANDS ARE RELATIVELY HIGH**

While about one in five UK-based organisations infected with ransomware saw ransom demands of no more than £350, most organisations saw demands significantly in excess of that figure, as shown in Figure 67. In fact, two in five UK-based organisations experienced ransom demands in excess of £3,500 and three percent were presented with demands in excess of £35,000.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{amounts_demanded.png}
\caption{Amounts Demanded by Ransomware Perpetrators}
\label{fig:amounts_demanded}
\end{figure}

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 4 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). Although ransomware in Germany may be less common than it is in other nations, it is significantly more expensive when it does occur.

\textsuperscript{10} http://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12
MOST RANSOMWARE VICTIMS OPT TO PAY

As shown in Figure 68, most UK-based organisations that fell victim to ransomware opted to pay the cybercriminals’ demands. Figure 69 reveals that organisations in the United Kingdom were the second most likely to pay, behind Canada, among the nations that we surveyed.

Figure 68
Was the Ransomware Paid?

Source: Osterman Research, Inc.
We attribute the greater propensity to pay ransomware demands partially to the fact that infections tend to be more widespread in British organisations than they are in the other nations surveyed, and that ransomware had much more of an impact on the ability of UK-based organisations in terms of their loss of revenue resulting from the attacks.
**MANY LOST FILES BY NOT PAYING**

As shown in Figure 70, by not paying cybercriminals’ ransom demands, nearly one-third of the UK-based organisations we surveyed that opted not to pay lost files as a result – about the same level of impact we saw in the United States.

Figure 70
Did Organisations Lose Files by Not Paying?

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 organisations 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, organisations 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).
IT SPENDS QUITE A LOT OF TIME REMEDIATING MALWARE

While a small number of UK-based organisations spend little time remediating the aftermath of a ransomware infection, one-third of them spent more than two person-days cleaning up after a ransomware infection, as shown in Figure 71. More than seven in 10 organisations spend more than one person-day doing so.

Figure 71
IT Staff Hours Spent on Remediation

Source: Osterman Research, Inc.
ORGANISATIONS IN THE UK ARE MORE FOCUSED ON TECHNOLOGY-CENTRIC APPROACHES

The ability to defeat ransomware must be a combination of robust technology and good user training, since the latter serve as a key line of defense against ransomware, particularly when its ingress point is through email. As shown in Figure 72, UK-based organisations lean toward a technology-centric approach in their efforts to thwart ransomware, although many place strong emphasis on user training, as well.

While U.S. organisations tend to lean a bit more toward training as a way to address the ransomware problem, organisations in the other nations we surveyed take a somewhat more technology-centric focus, with the United Kingdom leading the way in this regard. For example, while only six percent of U.S. organisations believe that dealing with ransomware is mostly a technology problem, this figure is much higher in the United Kingdom (35 percent), Germany (22 percent), and Canada (27 percent).
MANY UK-BASED ORGANISATIONS ARE NOT TRAINING-FOCUSED

As shown in Figure 73, many organisations in the United Kingdom do not offer ransomware training to end users – among those that currently do not, most do not have any plans to do so. Our research also found that among the nations surveyed, users in UK-based organisations were the most likely to receive training about ransomware only when they joined the company.

Figure 73
Current Level of Training Provided to Employees About Ransomware

![Bar chart showing the current level of training provided to employees about ransomware.](source)

Source: Osterman Research, Inc.

Interestingly, and consistent with the more technology-focused anti-ransomware approach in many UK-based organisations, British users are the least likely to receive continuous training with regard to detecting and preventing ransomware.
**A VARIETY OF ANTI-RANSOMWARE TOOLS ARE IN PLACE**

UK-based organisations have implemented a variety of tools to either detect or recover from a ransomware attack, as shown in Figure 74. Chief among these are cloud-based backups so that endpoints can be recovered to a known, good state after an attack; and on-premises backups. UK-based organisations were the most likely to have deployed ransomware-detection solutions in the cloud among the nations we surveyed, but least likely to have on-premises data backup solutions in place.

**Figure 74**
Tools in Place to Address Ransomware

<table>
<thead>
<tr>
<th>Tool Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular cloud-based backup to restore to a known good state</td>
<td>54%</td>
</tr>
<tr>
<td>Regular on-premises data backup to restore to a known good state</td>
<td>52%</td>
</tr>
<tr>
<td>Network segmentation</td>
<td>48%</td>
</tr>
<tr>
<td>Air gaps between data stores and the Internet</td>
<td>33%</td>
</tr>
<tr>
<td>Ransomware-detection solutions on-premises</td>
<td>27%</td>
</tr>
<tr>
<td>Ransomware-detection solutions in the cloud</td>
<td>20%</td>
</tr>
</tbody>
</table>

*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 Germany and the United States. Air gaps among UK-based organisations are quite common, but on-premises ransomware-detection solutions are less common among UK-based organisations than they are in the United States.
SIGNIFICANT INTEREST IN SOLVING THE RANSOMWARE PROBLEM
As shown in Figure 75, UK-based organisations place a significant priority on addressing ransomware issues – 55 percent place a high or very high priority on the general topic of “addressing the ransomware problem”, while one-half of the organisations we surveyed place this high a priority on investing in resources and technology to solve the problem. Not surprisingly, the greater technology focus on dealing with ransomware in the United Kingdom, only about one-third of UK-based organisations place a high or very high priority on investing in education and training to address the problem.

Figure 75
Priority for Addressing Ransomware Issues
Percent Indicating a High Priority or Very High Priority

<table>
<thead>
<tr>
<th></th>
<th>55%</th>
<th>50%</th>
<th>35%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing the ransomware problem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investing in resources, technology and funding to address ransomware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investing in education and training about ransomware for your end users</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

U.S. organisations 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. organisations, 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. organisations 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. organisations 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.
EXECUTIVE SUMMARY - GERMANY

KEY TAKEAWAYS

• Only 12 percent of corporate decision makers in German organisations consider ransomware to be a “concern” or “extreme concern”.

• Nearly 65 percent of organisations have been the victim of a cyber attack during the past 12 months, but only 18 percent have been the victim of a ransomware attack.

• The most heavily targeted industries for ransomware are healthcare and financial services.

• Decision makers in German organisations have a relatively high level of confidence in their ability to effectively stop ransomware: 14 percent of German organisations are “very confident” in their ability to stop ransomware attacks and another 52 percent are “fairly confident”.

• Nearly 75 percent of German organisations breached have had high-value data held for ransom. Most of the victims of ransomware in German organisations were mid-level or C-level managers.

• German organisations are only modestly committed to solving the ransomware problem: about one in five organisations are committed to addressing the ransomware problem as a “high” or “very high” priority, while about one in eight give this level of priority to investing in resources, technology and funding to address the problem. This is lower than in the U.S., but we believe this is only the result of the relatively low penetration of ransomware in Germany organisations.

• Ransomware attacks among German organisations have a relatively significant impact: nearly two-thirds of successful ransomware attacks are able to reach up to 25 percent of endpoints.

• Globally, nearly 40 percent of ransomware victims paid the ransom.

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 German organisations. The survey was conducted during June 2016 with 165 organisations 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 organisation. A total of 21 questions were included in the online survey. Results from the other surveys are available in separate survey reports. The distribution of industries surveyed in Germany is shown in Figure 76.

The 125 surveys conducted for this report provide a representative and statistically valid sample for purposes of drawing conclusions about the state of ransomware and other security-related issues among business and government organizations in Germany. While the largest possible sample is always preferable, this sample size is sufficient to draw meaningful conclusions from the data.

Figure 76
Distribution of German Industries Surveyed

<table>
<thead>
<tr>
<th>Industry</th>
<th>%</th>
<th>Industry</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>22%</td>
<td>Transportation</td>
<td>3%</td>
</tr>
<tr>
<td>Financial services/banking/insurance</td>
<td>14%</td>
<td>High tech</td>
<td>2%</td>
</tr>
<tr>
<td>Retail/eCommerce</td>
<td>8%</td>
<td>Pharmaceutical</td>
<td>2%</td>
</tr>
<tr>
<td>Engineering/construction</td>
<td>7%</td>
<td>Energy/utilities</td>
<td>2%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>6%</td>
<td>Food/agriculture</td>
<td>2%</td>
</tr>
<tr>
<td>Education</td>
<td>6%</td>
<td>Law enforcement</td>
<td>2%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5%</td>
<td>Other</td>
<td>14%</td>
</tr>
</tbody>
</table>
SURVEY FINDINGS

During the previous 12 months, 65 percent of German organisations surveyed have suffered a security attack, as shown in Figure 77. The majority of the organisations that were infiltrated have experienced a relatively low number of attacks. Interestingly, more than a third of organisations have not suffered a single attack in the previous 12 months, a much lower figure than in the United States.

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. organisations are the most attacked among the organisations that we surveyed and German organisations are attacked the least. For example, as shown in Figure 78, between 28 percent and 35 percent of the organisations in the nations we surveyed reported no security-related attacks during the previous 12 months versus 21 percent for U.S. organisations. At the other end of the scale, 22 percent of U.S. organisations reported that they had received more than 20 attacks during the previous year compared to between 8 percent and 10 percent for organisations in the other nations surveyed.
Table 7.1: Ransomware Attacks During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>21%</td>
<td>28%</td>
<td>35%</td>
<td>28%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>13%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>10%</td>
<td>20%</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>5%</td>
<td>30%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>More than 20</td>
<td>22%</td>
<td>9%</td>
<td>10%</td>
<td>10%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*

**Ransomware Attacks Are Comparatively Few**

As shown in Figure 7.9, the vast majority of the German organisations surveyed have not experienced a single ransomware attack during the past 12 months. Of those organisations that have experienced such an attack, it has been minimal – a maximum of five ransomware attacks.

Figure 7.9

Ransomware Attacks During the Previous 12 Months

Our research found that Canadian and German organisations experience significantly fewer ransomware attacks relative to U.S. organisations, but that those in the United Kingdom experience ransomware attacks to a slightly greater degree – 54 percent of organisations in the United Kingdom have experienced ransomware attacks compared to 47 percent in the United States, as shown in Figure 7.80. 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.

It is important to note, however, that ransomware is a serious problem in Germany despite the relatively low penetration of ransomware in our sample. For example, two German hospitals were victims of ransomware in early 2016, and so German organizations are clearly not immune from ransomware attacks to any greater degree than organizations in other nations.

**Figure 80**
Ransomware Attacks That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>USA</th>
<th>Canada</th>
<th>Germany</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>53%</td>
<td>65%</td>
<td>82%</td>
<td>46%</td>
</tr>
<tr>
<td>1 to 5</td>
<td>41%</td>
<td>27%</td>
<td>18%</td>
<td>42%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>4%</td>
<td>7%</td>
<td>0%</td>
<td>8%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>More than 20</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*

**THE IMPACT OF RANSOMWARE IS SIGNIFICANT**

When ransomware strikes German organisations, the impact can be significant. As shown in Figure 81, the largest single impact was on individual being impacted through the loss of files, loss of productivity and the like.

**Figure 81**
Values of the Files That Were Encrypted

- People were personally impacted (customers, students, vendors, staff, etc.) - 74%
- We lost revenue - 22%
- It stopped business immediately - 13%
- Employees used personally owned smartphones, tablets or laptops because corporate systems were down - 9%
- Lives were at stake - 4%

*Source: Osterman Research, Inc.*
More than one in five German ransomware victims lost revenue as a result of the infection, a much higher proportion than in the United States, but less than in either the United Kingdom or Canada. However, German organisations were more likely to report that a ransomware infection stopped business immediately, indicating the severity of ransomware among German organisations when attacks are successful.

**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 82, 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.

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 organisations 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 organisations in these industries, particularly for highly targeted, spearphishing-like attacks.
GERMAN ORGANISATIONS EXPRESS CONFIDENCE IN STOPPING RANSOMWARE

The majority of German organisations surveyed are fairly to very confident in their ability to stop ransomware, as shown in Figure 83. Roughly one-third of respondents are minimally confident in their ability to stop ransomware.

Interestingly, German organisations, along with their Canadian counterparts, are the most confident about their ability to stop ransomware. We attribute this to a couple of things: first, German organisations have a relatively low infection rate from ransomware relative to the other nations we surveyed; and second, German organisations train their users about how to deal with ransomware to a much greater extent than organisations in the other nations we surveyed.

Source: Osterman Research, Inc.
RANSOMWARE IS NOT A CRITICAL AREA OF CONCERN...YET
Email is the primary security-related problem in Germany, with almost 70 percent of organisations responding as concerned or very concerned about malware infiltration and phishing through email, as shown in Figure 84. Ransomware seems to be a minimal concern, with only 12 percent stating they are concerned or extremely concerned about it as a security-related problem.

Figure 84
Concerns About Security-Related Problems
Percent Responding Concerned or Extremely Concerned

<table>
<thead>
<tr>
<th>Security-Related Problem</th>
<th>Percent Concerned or Extremely Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infiltration through email</td>
<td>43%</td>
</tr>
<tr>
<td>Phishing through email</td>
<td>26%</td>
</tr>
<tr>
<td>Malware infiltration via web browsing</td>
<td>23%</td>
</tr>
<tr>
<td>Phishing through social media</td>
<td>14%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>12%</td>
</tr>
<tr>
<td>Insider theft of data</td>
<td>5%</td>
</tr>
<tr>
<td>Physical theft of laptops and mobile devices</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

While ransomware is the fourth highest security-related concern about which we queried in the survey of U.S. organisations, the level of concern about ransomware is higher in the U.S. than in the other nations we surveyed, but the lowest in Germany. For example, 50 percent of organisations 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 85. We attribute this low level of concern to the currently low ransomware penetration rate in German organisations, but one that could change in a short period of time.
Figure 85
Concerns About Various Security-Related Threats

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

Source: Osterman Research, Inc.

It is important to note, however, that U.S. organisations 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 ARE THE PRIMARY INGRESS POINT FOR MALWARE

Among organisations that have experienced a ransomware attack, roughly three-quarters have encountered the attack through a desktop computer. As shown in Figure 86, servers are also notable locations in which ransomware entered the organisation, and 13 percent of organisations is not sure of the source.

German organisations reported the highest level of ransomware infection via desktop computers among the nations we surveyed, as well as the highest level of infection through servers. Moreover, organisations in Germany reported much lower ransomware ingress through laptops or mobile devices. By contrast, U.S. organisations 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 0 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, 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. 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).

Source: Osterman Research, Inc.

---

11 http://www.statisticbrain.com/computer-sales-statistics/
It is also important to note that while laptops were not identified as an ingress point for malware in our German sample, the reader should understand that laptops represent a serious threat for ransomware infiltration. German organizations, like the others in our various national surveys, are heavy users of laptops.

**EMAIL IS A MAJOR THREAT VECTOR FOR RANSOMWARE**

As shown in Figure 87, email links and email attachments are the primary avenues by which ransomware enters German organisations. Non-email and non-social media web sites or web applications are also common entry points, but roughly one in three decision makers imply they don’t know the applications by which ransomware enters the organisations.

![Figure 87](image)

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email link</td>
<td>43%</td>
</tr>
<tr>
<td>Email attachment</td>
<td>17%</td>
</tr>
<tr>
<td>A Web site or Web application other than email or social media</td>
<td>4%</td>
</tr>
<tr>
<td>Social media</td>
<td>0%</td>
</tr>
<tr>
<td>USB stick</td>
<td>0%</td>
</tr>
<tr>
<td>Business application</td>
<td>0%</td>
</tr>
<tr>
<td>We don’t know</td>
<td>35%</td>
</tr>
</tbody>
</table>

*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 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.
RANSOMWARE IN GERMANY IMPACTS MANY ENDPOINTS

As shown in Figures 88 and 89, when ransomware infects endpoints in German organisations, the impact can be significant. While one in six organisations reported that ransomware infections spread to fewer than one percent of endpoints, nearly two-thirds of organisations report that they spread to as many as 25 percent.

Figure 88
Proportion of Endpoints to Which Ransomware Attacks Spread

Source: Osterman Research, Inc.
Figure 89
Endpoints Impacted by Ransomware Attacks

Source: Osterman Research, Inc.

While more organisations in the United Kingdom saw the spread of ransomware to 100 percent of the endpoints once they were infected, German organisations were also significantly impacted by ransomware: nearly one in five German organisations reported that malware infections impacted more than 25 percent of the endpoints on the network.
HIGHER LEVEL ROLES ARE IMPACTED
As shown in Figure 90, mid-level managers and C-level or other senior executives combined are quite heavily impacted by ransomware. Combined, these roles are much more impacted by ransomware infections than lower level staff members, such as clerical staff.

Figure 90
Roles Impacted by Ransomware Attacks

<table>
<thead>
<tr>
<th>Role</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower level staff members/clerical staff</td>
<td>14%</td>
</tr>
<tr>
<td>Mid-level managers</td>
<td>13%</td>
</tr>
<tr>
<td>C-level or other senior executives</td>
<td>6%</td>
</tr>
<tr>
<td>External staff (e.g., consultants, contractors, vendors etc.)</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

U.S. organisations see a much greater impact from ransomware on lower level staff members than do organisations in Germany and 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. organisations also see much greater impacts from ransomware on C-level and other senior executives (25 percent in the United States compared to 6 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 9 percent in Germany, as shown in Figure 91.
Figure 91
Roles That Have Been Impacted by Ransomware

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

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. 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 5 percent to 20 percent — and the rest goes to the ‘script kiddie’ who deployed the attack."

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.

GERMAN RANSOM DEMANDS ARE HIGH

The amounts demanded by cybercriminals in German ransomware attacks are significantly higher than in the other nations we surveyed. As shown in Figure 92, nearly one-half of ransomware demands are in excess of €9,100.

Figure 92
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 4 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). Although ransomware in Germany may be less common than it is in other nations, it is significantly more expensive when it does occur.
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 Figures 93 and 94. On average, 22 percent of German organisations pay the ransom demanded after they are infected, the second lowest payment rate of the nations we surveyed.

Figure 93
Was the Ransomware Paid?

Source: Osterman Research, Inc.
However, the proportion of German organisations 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 organisation will be to pay the ransom demands.
MANY LOST FILES BY NOT PAYING THE RANSOM

As shown in Figure 95, one in nine German organisations that chose not to pay the ransom demands lost files as a result of their decision. However, this is the lowest rate of lost files among the nations we surveyed for those who chose not to pay the cybercriminals’ ransom demands.

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 organisations 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, organisations 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).
IT REMEDIATION TIME EXPENDITURES ARE SIGNIFICANT

While a small handful of German organisations spend relatively little time remediating the aftermath of a ransomware infection, nearly two in five organisations spent more than two person-days cleaning up after a ransomware infection, as shown in Figure 96. The vast majority of organisations spend more than one person-day doing so.

Figure 96
IT Staff Hours Spent on Remediation

Source: Osterman Research, Inc.
THE BALANCE OF 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 97, German organisations view ransomware prevention and remediation as focused on both training and technology and have struck a reasonable balance between the two.

Figure 97
Preferred Balance Between Training and Technology to Address the Ransomware Problem

While U.S. organisations tend to lean a bit more toward training as a way to address the ransomware problem, organisations in the other nations we surveyed take a somewhat more technology-centric focus. For example, while only 6 percent of U.S. organisations 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). Among the nations we surveyed, German organisations have the most balanced view between addressing ransomware through training vs. technology.
GERMAN ORGANISATIONS OFFER THE MOST TRAINING

Our research found that German organisations were far more likely than those in the other nations we surveyed to provide continuous ransomware training to their users. As shown in Figure 98, more than one-half of German organisations provide more or less continual training, while only six percent of organisations do not provide any form of training.

Figure 98
Current Level of Training Provided to Employees About Ransomware

The much greater degree to which ransomware training is provided in German organisations may go a long way toward explaining why ransomware infections in Germany are lower than in other nations. Because users are more accustomed to receiving training on what ransomware looks like and how to avoid it, they may be a more effective first line of defense than users in other nations.
## BACKUPS ARE COMMON DEFENSE AGAINST RANSOMWARE

As shown in Figure 99, that vast majority of German organisations use regular, on-premises data backup solutions as a way to remediate the impact of a ransomware attack. Network segmentation is also commonly used to help mitigate the spread of ransomware infections once they occur.

### Figure 99
Tools in Place to Address Ransomware

<table>
<thead>
<tr>
<th>Tool</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular on-premises data backup to restore to a known good state</td>
<td>87%</td>
</tr>
<tr>
<td>Network segmentation</td>
<td>74%</td>
</tr>
<tr>
<td>Air gaps between data stores and the Internet</td>
<td>32%</td>
</tr>
<tr>
<td>Ransomware-detection solutions on-premises</td>
<td>19%</td>
</tr>
<tr>
<td>Regular cloud-based backup to restore to a known good state</td>
<td>6%</td>
</tr>
<tr>
<td>Ransomware-detection solutions in the cloud</td>
<td>2%</td>
</tr>
</tbody>
</table>

*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 Germany and the United States. Air gaps among U.S. organisations are used much less often than in the other nations, but on-premises ransomware-detection solutions are much more common in the United States. However, German organisations were the most likely among the nations we surveyed to use regular, on-premise data backups and network segmentation as tools to mitigate the impact of ransomware.
THE FOCUS ON RANSOMWARE IN GERMANY IS LOW

German organisations do not seem to place a high priority on addressing ransomware issues. As seen in Figure 100, only one in five place a priority on addressing the ransomware problem, and even fewer than that want to invest in resources and education to solve these issues.

Figure 100
Priority for Addressing Ransomware Issues
Percent Indicating a High Priority or Very High Priority

<table>
<thead>
<tr>
<th>Priority</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing the ransomware problem</td>
<td>19%</td>
</tr>
<tr>
<td>Investing in resources, technology and funding to address ransomware</td>
<td>13%</td>
</tr>
<tr>
<td>Investing in education and training about ransomware for your end users</td>
<td>9%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

U.S. organisations 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. organisations, 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. organisations 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. organisations 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 9 percent in Germany.

Here again, Osterman Research believes that the low interest in addressing ransomware among German organisations is a direct result of the relatively low infection rate among these organisations. If (and probably when) ransomware becomes much more common in Germany, we anticipate that interest in addressing the problem will increase quickly.
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.

© 2016 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.