Ransomware Revealed: Paying for the Protection of your Privacy

A study on the awareness and perception of ransomware attacks in businesses across North America

kaspersky

Introduction

As cybercriminals continue to improve their methods of stealing private information for financial gain, ransomware is becoming a popular attack vector for businesses of all sizes and industries in North America.

According to Kaspersky, research experts observe that roughly 900,000 to almost 1.2 million of all users are targeted by ransomware every six months. This means that cybercriminals are increasing the precision of their targeting to locate victims with security breaches in their defense systems, and business organizations are feeling the financial impact.

A 2019 report from EMSISOFT found that ransomware attacks impacted at least 966 government agencies, educational establishments and healthcare providers. A further breakdown shows 113 state and municipal governments and agencies, 764 healthcare providers and 89 universities, colleges or school districts were impacted by ransomware.

When considering publicly available information, ransom amounts have varied greatly with attacks costing $1,032,460 on average, and highs reaching up to $5,300,000. However, the long term consequences following a ransomware attack can be far more devastating when considering the disruption to essential corporate networks and the costs associated with rebuilding an organization's IT infrastructure.

To gain a better understanding of how employees at business organizations perceive ransomware, Kaspersky commissioned a survey to gauge their sentiments and further explore the potential reasons why ransomware attacks are drastically on the rise.

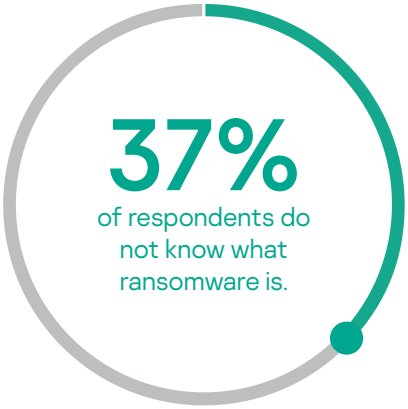
In sharing the results of the complete survey data, Kaspersky aims to create an open dialogue among businesses and their employees about the current level of awareness in regards to ransomware attacks and how, through awareness, the risk of future attacks can be mitigated. Additionally, the report offers suggested proactive tips on how management personnel, particularly those who involved with IT, can prioritize cybersecurity awareness so that all employees feel confident in championing their personal information as well as their organization's information.

Key findings from the study include:

- **On average across the US and Canada, 45% of respondents wouldn't know what steps to take in response to a ransomware attack.**
- **In North America, just over two thirds (67%) of respondents would not be willing to pay anything to recover personal digital files or devices they could no longer access if they fell victim to a ransomware attack.**
- **On average, 39% of all respondents think that companies should pay a ransom to retrieve personal information about employees.**
- **Across the US and Canada, over two thirds (68%) of respondents think that IT security should be most responsible for safeguarding private employee information.**
- **In North America, more than a third (35%) of respondents wouldn't know what to do if an organization didn't pay the ransom and their personal information was at stake.**

Research Methodology

This quantitative study was conducted by research firm Opinion Matters via an online survey targeting 2,007 business employees aged 17 and older from the United States and 1,011 employees of the same age from Canada on their knowledge of ransomware in the workplace. The survey was conducted in November 2019. Not all survey results are included in this report.



Research Findings

Defining Ransomware

Upon conducting this survey, it was important to first have an understanding of respondents' knowledge about the term ransomware, which is defined as when a computer system is held to ransom, restricting access to files and demanding the user pays a ransom to remove the restriction. The findings from asking this question concluded that, on average, 37% respondents do not know what ransomware is, highlighting that a significant amount of business employees lack basic knowledge and awareness about this type of cyber threat.

3 in 10
respondents who have experienced a ransomware attack still responded that they do not know what ransomware is.

Even more alarming, however, was that over 3 in 10 (32%) respondents who have experienced a ransomware attack still responded that they do not know what ransomware is, further proving that such an incident did not influence employees to learn more about how to prevent future cybersecurity incidents that their organization could be prone to.

As the remainder of the survey results will conclude, **lack of awareness** about ransomware, what it is, what it does and who is responsible for preventing such an incident from occurring will be a common theme throughout the report.

What to Do in Case of a Ransomware Attack

In the unfortunate chance that an organization is hit with ransomware, it is imperative that employees have an understanding of the immediate next steps to take in order to inform the appropriate parties, and more importantly, mitigate any further risk.

When posing this question in the survey, more than a third (35%) of respondents in North America admitted that they would not know what to do if their business organization did not pay a ransom and their personal information was at risk of being exposed.

Since many respondents do not know the proper steps to take when hit with a ransomware attack, the seemingly obvious answer to counter an attack could be to simply pay the ransom. Results from the survey found that over 1 in 5 (21%) respondents who have experienced a ransomware attack think an organization should never pay the ransom, versus under 1 in 7 (15%) who have not experienced a ransomware attack.

When consulting Kaspersky's research experts, they stand firm in their position that paying a ransom is not the best way to stop an attack as it does not guarantee that private information will remain undisclosed.

How does this advice stack up against how our survey respondents answered? Reactions from respondents in the U.S. and Canada had similar views, 31% and 28% respectively, saying an organization should use a ransomware decryption tool, and 5% and 4% respectively, think employees should offer to pay the ransom if an organization does not pay the ransom and employee information is at stake.

While these numbers do not represent the majority, it does pose a cause for concern that employees think these are appropriate actions to take, and further highlights the need for awareness about best practices when responding to a ransomware attack.

"It is clear that ransomware as an attack strategy is on the rise, and businesses as well as employees must be vigilant in spotting potential attacks to safeguard private information.

When it comes to the question of paying a ransom, our recommendation is to never pay a ransom, and there are a few reasons for this. First, paying a ransom will never guarantee that all of your data will be returned – it might be partially returned or not at all. There is also no way to tell if your information has been sold in underground markets once obtained.

Second, paying a ransom only encourages cybercriminals to further carry out these attacks as they are one of the most financially profitable attacks malefactors can perform. The more business organizations give in to ransomware attacks, the more we will see them continue to trend in the threat landscape."

Brian Bartholomew,
Principal Security Researcher,
Global Research and Analysis Team
Kaspersky North America.

How to Stop a Ransomware Attack

Now that it is clear that paying a ransom does not necessarily mean that IT systems will automatically resume normal operations and private information may not be completely restored, the next logical question is how to stop a ransomware attack from occurring.

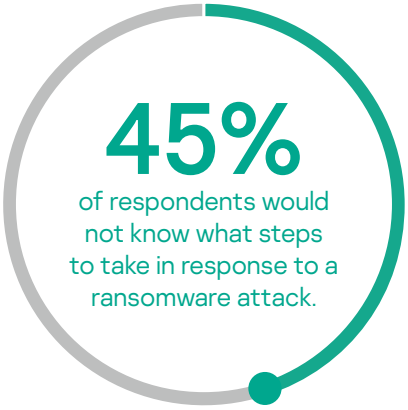
Across the U.S. and Canada, 45% of respondents would not know what steps to take in response to a ransomware attack. What's more, for the respondents who have previously experienced a ransomware attack, 2 in 5 respondents (40%) also responded as such.

Additionally, 30% of people who have experienced a ransomware attack appropriately responded that disconnecting a computer from the internet would be the best first step to take stop an attack, versus 22% of respondents who have not experienced a ransomware attack. In addition to disconnecting from the internet, Kaspersky experts recommend disconnecting the infected computer from any networks to isolate unit and prevent the malware from spreading.

The survey also found that more than two thirds (67%) of respondents think that a company should locate the threat and rectify the problem versus 1 in 12 (8%) of respondents who think there are no appropriate plans of action a company should follow with a ransomware attack.

Some additional helpful tips employees can consider when it comes to prevention of a ransomware attack include:

- **Never click on unverified links**
- **Only open attachments from trusted email attachments**
- **Download from trusted sites only**
- **Install trusted security software like Kaspersky Internet Security on your devices**



"Increasingly, employees have an opportunity to participate in ransomware prevention either by attending security awareness training sponsored by the companies in which they work or independently by doing minimal research and consuming just a few basic online training courses, mostly available at no cost.

Ultimately, employers and custodians of the data are responsible to assure that all of the preventive and recovery measures are in place and that essential controls exist within a secured environment to both deter and detect as well as remedy a ransomware attack."

Steve King,
Cybersecurity Advisory Services Director,
Information Security Media Group and CyberTheory, and former CISO for Wells Fargo Bank

Who is Responsible, and How Much Do you Trust Them?

Although a significant number of employees are unaware of the fundamentals of ransomware, survey respondents are largely in agreement (68%) that IT security teams should be held most responsible for safeguarding private employee information by having the proper security protections in place. Alternatively, 5% of respondents think individual employees should be responsible for safeguarding private employee information by way of more carefully checking links, attachments, etc. before opening them.

Trust is also a key factor in how much employees feel their organization is prioritizing private information, as well as how capable they are of apprehending a ransomware attack. Overall, men were more trusting with 1 in 10 (10%) male respondents versus 1 in 14 (7%) females respondents reporting they have complete trust that their organization will keep private information safe and successfully stop a ransomware attack.

When further breaking down demographics by age, respondents in the Gen Y generation are more trusting with over three quarters (77%) of respondents saying that have complete trust or some trust versus over two thirds (67%) of respondents born in the Baby Boomer generation who responded the same when it comes to how much they trust their organization to keep their private information safe.

When it comes to geography, the U.S. is slightly more trusting with 9% of respondents have complete trust compared to 6% of respondents in Canada.

Best Practices for Ransomware Incident Response

Once a ransomware attack strikes, it is important to take the proper steps when communicating the incident to both the public and employees. The Cybersecurity and Infrastructure Security Agency (CISA) recommends reporting the incident to their team immediately. Among the advantages of centralized reporting is the possibility that organizations will learn how other have been able to effectively respond to similar attacks, and whether there are methodologies for successfully decrypting a particular strain of ransomware without having to pay the attacker. The downside to reporting a ransomware attack may result in decreased customer and shareholder confidence in an entity's overall information security posture.

More than 3 in 10 (32%) respondents feel the public should be notified as soon as an attack occurs, versus 45% of respondents who think the employees should be notified first. Alternatively, 5% of respondents feel as though no information about a ransomware attack should be revealed. When it comes to internal communications, 46% of respondents think employees should be notified straight away versus 2% who feel the information should be kept under wraps from personnel.

"Whether and how a ransomware attack should be reported often depends on the nature and circumstance of the attack, the nature of the system attacked, the nature of the data on that system and who you are reporting it to and why. If the ransomware attack methodology indicates unauthorized access to computers, systems or data which contains Personally Identifiable Information (PII) data breach disclosure laws may require reporting the incident either to authorities, to the data subjects affected or both.

Similarly, if you are holding data for a third party your contracts or SLA's with these third parties may require disclosure of security 'incidents' which might impair your ability to protect that data or to ensure its availability. Reporting to organizations like Computer Emergency Response Centers (CERTs) or Information Sharing and Analysis Centers (ISACs) may enhance readiness and response and provide you or others with critical data to respond.

Reporting to technical coordinating entities (including IR vendors, software and cloud vendors and suppliers) may help to understand the nature of the attack and responses. Reporting to various threat intelligence entities may help to learn about the nature and motivations (and history) of the specific threat actors involved. Finally, many entities – even when not required to do so – will report and coordinate their responses with state, local, federal and international law enforcement agencies including the FBI's Internet Crime Complaint Center (IC3) or various InfraGuard chapters."

Mark Rasch,
Cybersecurity and privacy attorney in Bethesda, MD

Putting a Price on Privacy

As is the case with most cyberattacks, the main purpose is financial gain; however, when it comes to the attack vector of ransomware, the sole purpose is financial gain. Given that private information, whether personal or business, is at stake, it begs the question of how much money individuals would be willing to spend to keep such information concealed.

The overwhelming response from the survey concluded that just over two thirds (67%) of respondents in North America would not be willing to pay any amount of money to recover personal digital files or devices they could no longer access if they fell victim to a ransomware attack.

Millennials born between the years of 1995 to 2002 were the most willing to pay for their privacy with 1 in 5 (20%) saying they would be willing to pay $50 to $200 to recover their information versus those born in 1964 or earlier who responded the same at only 7%.

When breaking this question down by geography, Canadians are less likely to pay to recover files. 7 in 10 (71%) respondents selected $0, as in they wouldn't be willing to pay anything to recover personal digital devices or files if they fell victim to a ransomware attack compared to 65% in the U.S.

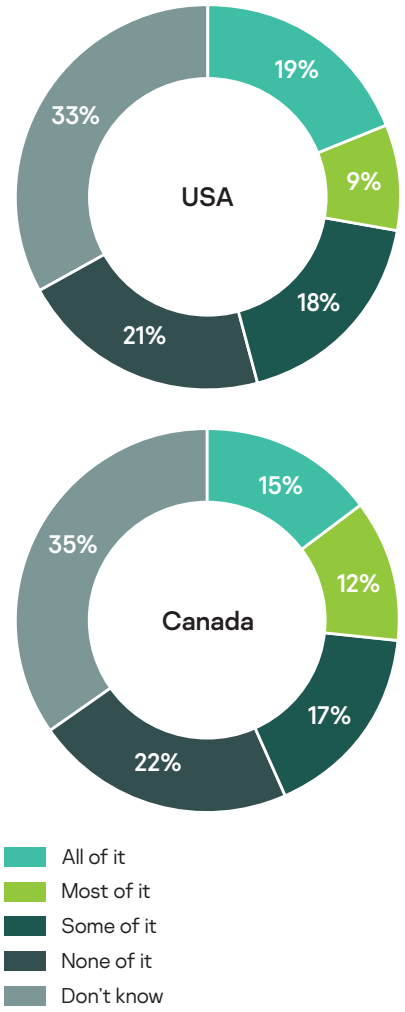
How do these numbers differ when it comes to the price employees think their organization should pay to retrieve private data? On average, 39% of respondents think that companies should pay a ransom to retrieve personal information about employees (such as telephone numbers, addresses etc.). What type of information was a top priority to retrieve? According to respondents in the U.S. (45%) and Canada (42%), it is social security numbers.

As we have previously discussed, paying a ransom does not guarantee that all of the information being withheld will be fully concealed. This was indeed the case in the most infamous ransomware attack of our time known as WannaCry, as researchers were never able to confirm that all systems were fully restored for users who paid the enforced ransom.

When asking respondents how much information they thought they might be able to retrieve after paying a ransom, over a third (34%) of respondents said they were unsure how much of their personal information they would get back.

Over 3 in 10 (31%) of respondents who have experienced a ransomware attack think that they would get back most or some of the personal information versus over 1 in 5 (21%) respondents who have not experienced a ransomware attack. Additionally, the U.S. (21%) and Canada (22%) agree in responding that they would not get any of their personal information back in exchange of paying a ransom.

If you were to pay a ransom in exchange for your personal information, how much of your information do you think you'd get back?



Looking Ahead

As we look ahead to the future of threat attacks in 2020, Kaspersky experts predict that we will continue to see a rise in ransomware attacks, particularly targeted at municipalities.

There are several reasons why cyber attackers will likely continue to target local governments this year including oversights in how cities allocate their cybersecurity budgets, the numerous IT networks that municipalities function on and the vitality of municipalities to function properly and at full capacity each day as to not disrupt the welfare of citizens.

Businesses and employees can do their part in minimizing ransomware attacks by following these guidelines:

- It is essential to install all security updates as soon as they appear. Most cyberattacks exploit vulnerabilities that have already been reported and addressed, so installing the latest security updates lowers the chances of an attack.
- Protect remote access to corporate networks by VPN and use secure passwords for domain accounts.
- Always update your operating system to eliminate recent vulnerabilities and use a robust security solution with updated databases.
- Keep fresh back-up copies of your files so you can replace them in case they are lost (e.g. due to malware or a broken device) and store them not only on a physical medium but also in the cloud for greater reliability.
- Remember that ransomware is a criminal offence, and you shouldn't pay a ransom. If you become a victim, report it to your local law enforcement agency. Try to find a decryptor on the internet first – some of them are available for free here: https://noransom.kaspersky.com.
- Educate employees about cybersecurity hygiene to prevent attacks from happening. Kaspersky Interactive Protection Simulation Games offers a special scenario that focuses on threats relevant to local public administration.
- Use a security solution for organizations in order to protect business data from ransomware. Kaspersky Endpoint Security for Business has behavior detection, anomaly control and exploit prevention capabilities that detect known and unknown threats and prevent malicious activity. A preferred third-party security solution can also be enhanced with the free Kaspersky Anti-Ransomware Tool.

This research highlights the need for more awareness around advanced threats such as ransomware, and best practices for knowing how to mitigate future risks. Kaspersky is committed to helping organizations understand the risks of cybersecurity and what is necessary to empower employees and protect businesses. Kaspersky will continue to research and investigate ransomware to further keep business organizations informed as to how they can protect against this threat.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at **usa.kaspersky.com**.

www.kaspersky.com