HACKING AMERICA: CYBERSECURITY PERCEPTION

A study on Americans' understanding of cybersecurity and hackers

hackerone

KASPERSKY lab

INTRODUCTION

Internet security is not only something that Americans have to be mindful of in their daily, personal lives, but also something that needs to be top-of-mind while at work.

Kaspersky Lab and HackerOne partnered to gain insight into U.S. consumers' perception of the hacker mindset, work and personal cybersecurity threats through a comprehensive survey. To gain this knowledge, Kaspersky Lab commissioned the research firm Opinion Matters to survey over 5,000 Americans in the United States, aged 16+.

The results take a broad look at what Americans think about hacker motivations, who they think security responsibilities fall on, whether or not America is more or less at risk with the new president and whether consumers trust their employers' efforts on cybersecurity and their stance on ransom payments.

Key findings from the study include:

- More than one in five (22%) U.S. adults said that they would be more likely to make a purchase if they knew a company hired hackers to help protect the security of their systems/devices/products they sell.
- U.S. adults think that retailers (73%) and credit payment companies (64%) should hold the majority of the responsibility when it comes to protecting their data for purchases they make online.
- Age also impacts American views on who is responsible for protecting their data online.
    - Young adults (25-43 years old) admitted that they, themselves, should take responsibility for protecting their own data when purchasing online (63%).
    - Americans 55 years and older were the most likely to say that the retailers should be responsible for the protection of their data when purchasing online (74%).
- 44% of U.S. adults believe that North America will be more vulnerable to cyber-espionage or nation-sponsored cyberattacks with Donald Trump as president of the United States.
- Only 36% of U.S. adults said that they would choose to be a customer of their own employer knowing what they know about their company's cybersecurity program and ability to protect customers from cyber criminals.
- When asked what types of data that if held for ransom they would expect a business to pay to get the data back, 43% of U.S. adults said employee social security numbers, customer banking details (40%) and employee banking details (39%).

RESEARCH METHODOLOGY

The quantitative study was conducted by research firm Opinion Matters via an online survey in December 2016 of 5,000 adults aged 16+ in the United States.

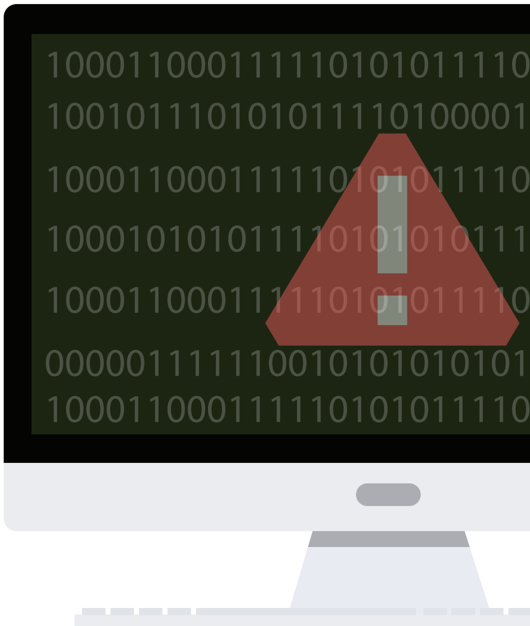
THE RESEARCH FINDINGS

Why Do Hackers Hack?

What motivates and drives someone to hack is often a mystery. It is quite difficult to pinpoint exactly why someone decides to hack a person, a business or government but regardless, it's certain that hackers can choose to do a lot of good or damage with the sensitive information they uncover, and in some cases, expose.

When U.S. adults were asked what they think motivates hackers, nearly four in five (79%) said that they think hackers are motivated by potential financial gain. When compared to HackerOne's "2016 Bug Bounty Hacker Report"[i] this isn't far off: 72% of hackers surveyed said they hack for money. The survey confirms that money is a major driver for hacking, whether hacking to help companies uncover flaws in their systems or hired to expose a business and their customers.

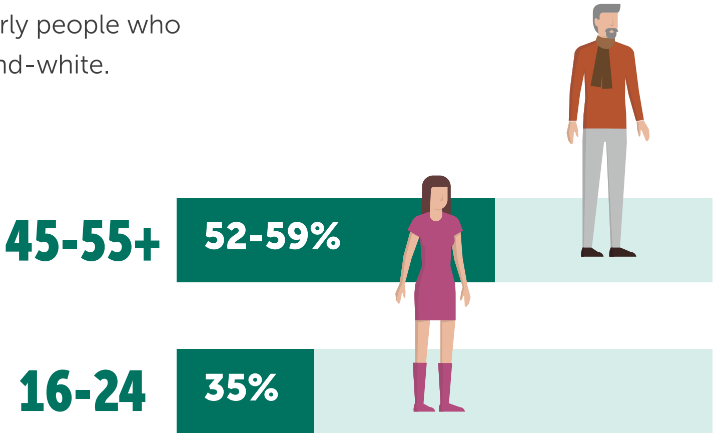
It's no surprise that most people would think that hackers are primarily motivated by financial gain, but the second top motivation, according to Americans, is morale boost. Nearly three in five (59%) Americans surveyed thought ego boosting was a motivation for hackers. When looking at some of the gender demographics, men were more likely than women to think an ego boost was a motivation for hackers (62% vs 56%). On the other hand, women felt stronger than men about thinking that the motivation for hackers comes from the desire to access personal data/information and hack into people's accounts (57% vs 50%).



In San Francisco, where the largest information security event takes place in February - RSA Conference - Americans gave hackers the benefit of the doubt and said that they believe they were mostly testing their skills. San Francisco residents were most likely to think that hackers were motivated by potential personal gain from outsmarting the technology (59%).

Despite the rise in news reports about the ethical hacking movement[ii], people still think of hackers in general as bad guys, particularly people who remember the '90s when hacking was portrayed as black-and-white.

When taking a look at age demographics, older generations (45-54 and 55+ years old) were more likely to believe hackers are up to no good with no positive incentives driving them. Older generations were the most likely to think that the motivation for hackers was to be malicious or create problems (52% and 59% respectively). To compare with attitudes among younger generations, only 35% of 16-24 year olds felt hackers hacked with malicious intentions.



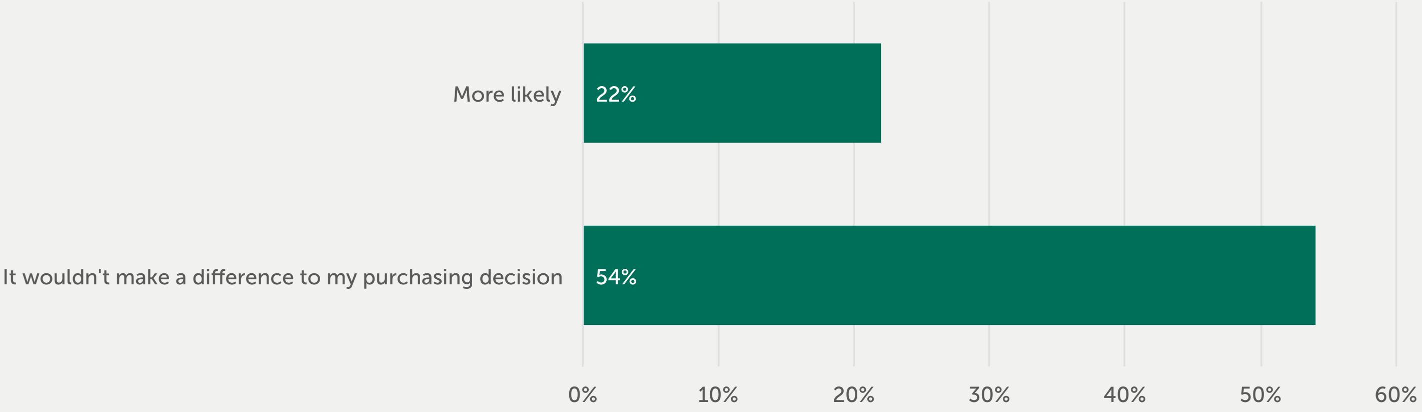
Hacking for Good?

While financial gains and mental self-validation are perceived to be key drivers, there are hackers in the information security community that aren't in it for personal gain, according to respondents. The survey found that 15% of Americans believe that hacking to protect others by reporting vulnerabilities was a motivation, and 14% think hackers are motivated by the good feeling they would get by helping companies or the government understand where the weaknesses are in their systems. This is often true and is why bug bounty programs are implemented by security-conscious organizations.

Bug bounty programs are a way for businesses to supplement the internal security work their team is doing by working with the global hacker community to find security vulnerabilities. In exchange for the security vulnerability, hackers are rewarded for their efforts and this is often called a bounty.[iii]

Hacking Isn't Changing Buying Behavior

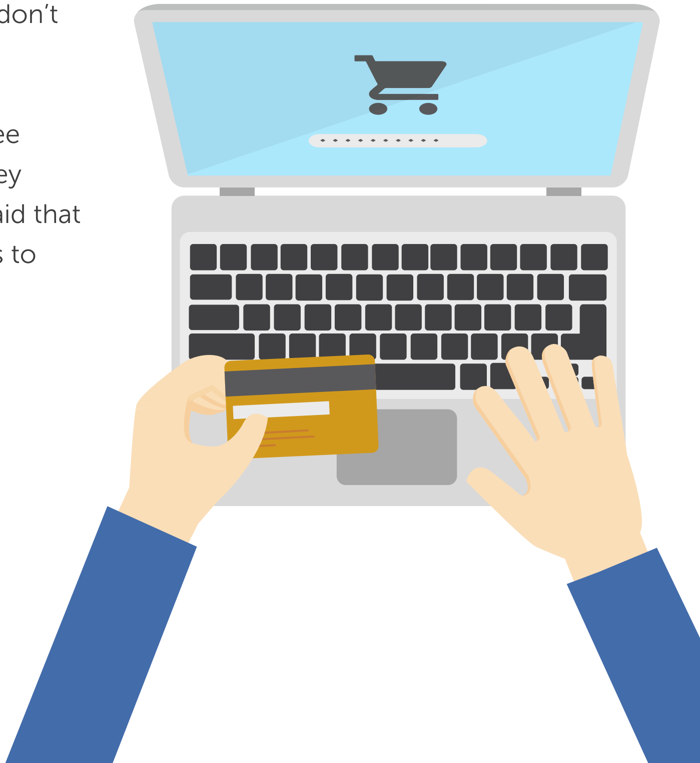
If you knew a company hired hackers to help protect the security of their systems/devices/products they sell, are you more or less likely to make a purchase?



Security professionals are well aware of the benefits of bug bounty programs, but as an emerging industry there is still work to be done to advance awareness and explain the value to Americans. That said, the results revealed that more than one in five (22%) U.S. adults feel safer patronizing companies that work with hackers to help improve the security of their systems/device/products they sell.

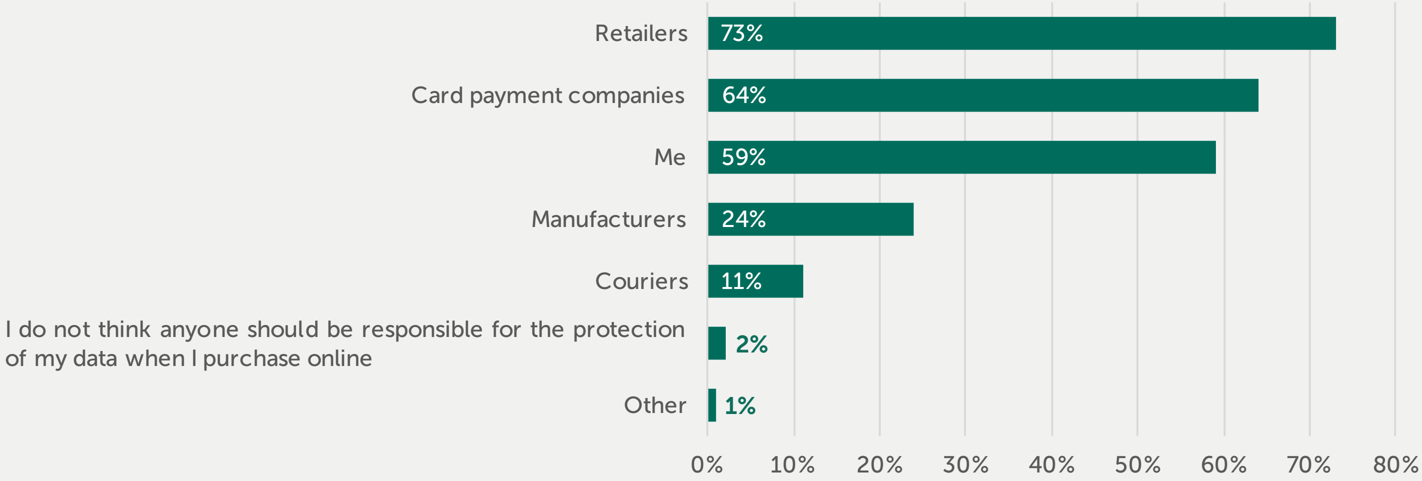
When taking a closer look at "hacking for good" from a generational standpoint, Americans ages 55 and older were the most likely to say that it wouldn't impact their purchasing decision (55%) if a company worked with hackers to improve security. This could be because they simply don't understand the benefits or don't care.

On the other hand, younger generations who are digital natives do see the value in a company hiring hackers to help protect the services they purchase. The results show that 29% of Americans 35-44 years old said that they were more likely to make a purchase if a company hired hackers to help protect the security of their systems/devices/products they sell.



Lacking an Understanding: Security as a Shared Responsibility

Who do you think should be responsible for the protection of your data when you purchase online?



The survey found that Americans are looking to others to own the responsibility for their security. When asked who should be responsible for the protection of their data when they make purchases online, 73% of survey participants said that retailers should be responsible, followed by credit payment companies at 64%. While the majority pointed to retailers and credit card companies, surprisingly, younger adults (25-43 years old) admitted that they, themselves, should take responsibility for protecting their own data when purchasing online (63%).

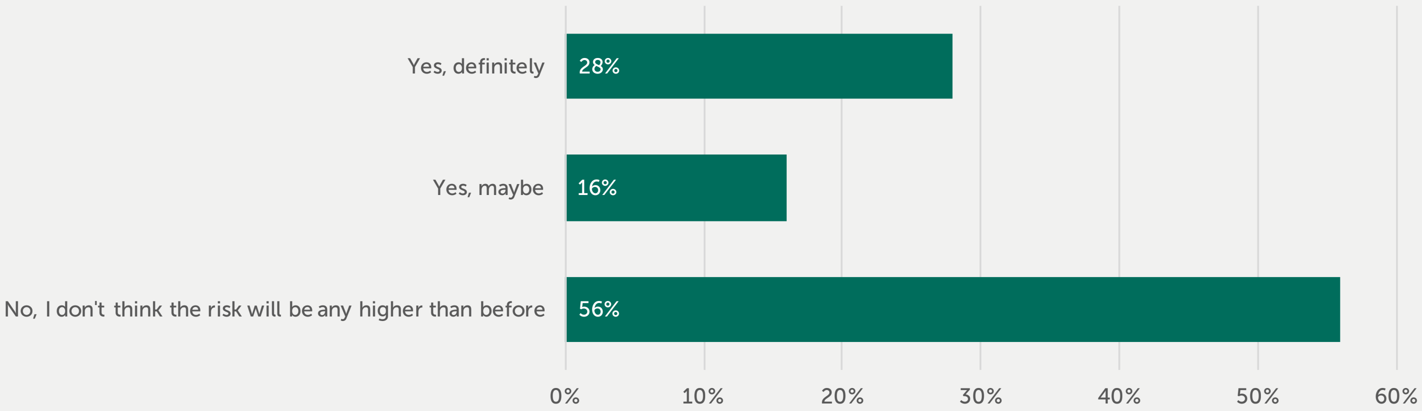
Respondents who were ages 55 and older in the U.S. were most likely to say that retailers should be responsible for the protection of their data when purchasing online (74%).

Although most vendors and retailers do have cybersecurity protections in place to help safeguard customers, consumers cannot rely solely on retailers to protect their personal information. Before shopping and banking online, Americans should educate themselves about cybersecurity, as well as have internet security software installed on their devices.

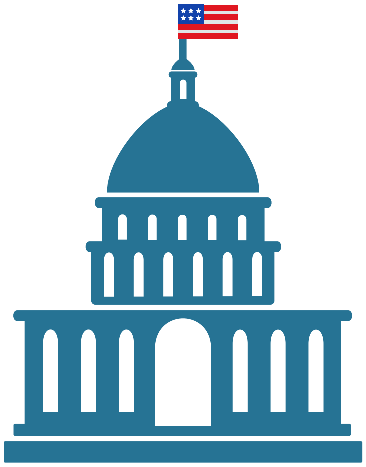
The State of Cybersecurity and Politics in the U.S.

Given the political divide in the country, the survey included a question to gauge public sentiment about the impact of the new president on cybersecurity protection and the American people.

Do you think North America will be more vulnerable to cyber-espionage or nation-sponsored cyberattacks with Donald Trump as President of the United States?



The research shows that America remains divided, with 44% of U.S. adults believing that under President Donald Trump, North America will be more vulnerable to cyber-espionage or nation-sponsored cyberattacks. Men are slightly less concerned than women (60% vs 52%) about the state of cybersecurity under the new administration.



So who is concerned? Young people ages 16-24 (millennials) in the U.S. were the most likely to think that North America would be more vulnerable to cyber espionage or nation-sponsored cyberattacks with Donald Trump as president (56%).

Business Perception: Trust and Employers

According to Kaspersky Lab's Corporate IT Security Risks Report 2016[iv], employees are one of the biggest cyberthreats to businesses in North America and in just the past year, 44% of these businesses have suffered four or more data breaches.

Businesses need to enforce cybersecurity awareness training in the workplace or the employee will continue to be a constant issue, continually putting sensitive customer, employee and proprietary data at risk.

Surprisingly, the majority of the participants in the survey actually don't trust their own employers with personal data. Only 36% of U.S. adults said that they would choose to be a customer of their own employer knowing what they know about their company's cybersecurity program and ability to protect customers from cyber criminals.

Knowing what they know about their employer's cybersecurity program and ability to protect customers from cyber criminals, women are slightly more trusting of their company's cybersecurity measures than men with 37% choosing to be a customer compared to 35% of American men.

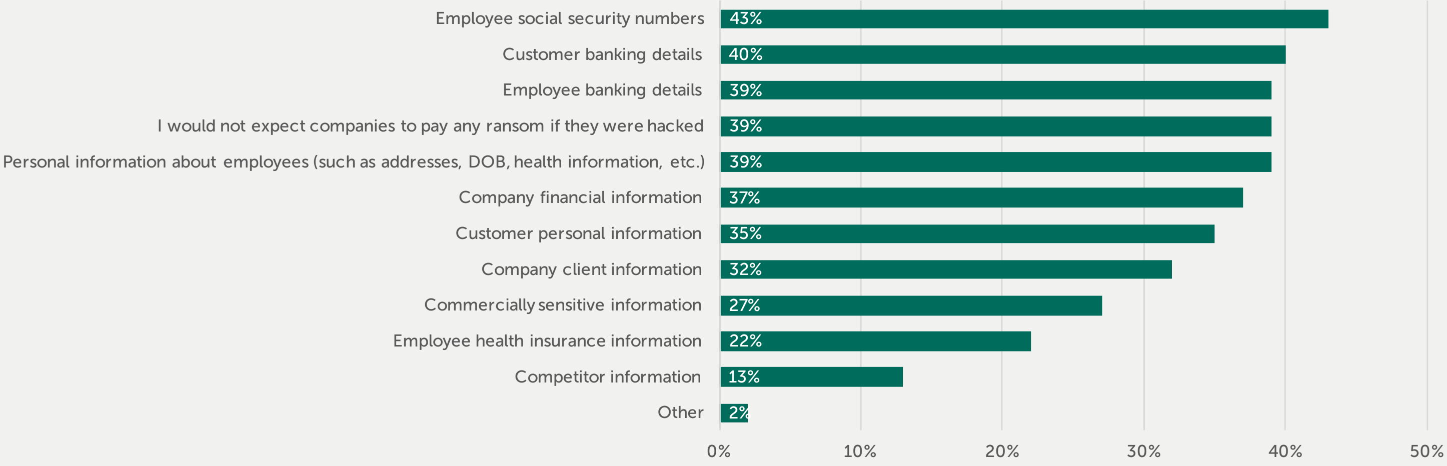
Businesses Perception: Ransomware Threats

Throughout 2016, ransomware has significantly increased – from an attack every two minutes in January, to one every 40 seconds by October according to Kaspersky Lab's Story of the Year report[v]. When a ransomware attack happens to a business, sensitive corporate and customer data is put in the hands of cybercriminals.

Ransomware is an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. If a company falls victim to a ransomware attack, they are locked out of their systems and expected to pay a ransom with no guarantee that the organization will actually get the data in return for its payment.[vi]

When asked what types of data Americans would expect a business to pay a ransom for to get the data back, the top answer was employee social security numbers (43%), followed by customer banking details (40%) and employee banking details (39%).

If a company fell victim to a cyberattack, what types of data would you expect them to pay a ransom to get back?



Compared to the Kaspersky Lab Ransomware Report 2016[vii], fewer Americans think companies should pay a ransom to get customer banking details back (Kaspersky Lab ransomware survey 2016: 57%, this survey: 40%), or to get customer personal information back (Kaspersky Lab ransomware survey 2016: 53%, this survey: 35%). Have people changed their perception of the business' responsibility regarding a ransom attack?

While nearly two in five (39%) U.S. adults said they would not expect the companies to pay any ransom if they were hacked, 34% of U.S. adults would expect companies to pay a ransom in order to get customer personal information back.

In addition, women were more likely than men to expect a company to pay a ransom if the company fell victim to a ransomware attack (63% vs 58%). The 45-54 year-olds surveyed were the least likely age group to expect a company to pay ransom if it was hacked (with 42% saying they would not expect the company to pay any ransom if hacked).

CONCLUSION

Despite the cybersecurity awareness efforts today of IT security companies, the government, businesses and more, there is still a lot of education needed to help transform Americans from a vulnerable state into a more cyber-secure society.

To begin, many Americans have a negative picture of what a hacker is and why they do what they do painted in their minds. While there are malicious hackers in the world, not all hackers are criminals, and the "good guys" don't get nearly enough recognition for their positive work benefitting society, for example bug bounty programs. The data shows that more than 1 in 5 Americans recognize the role hackers can play in protecting "consumers" online and recognize the value in pioneering cybersecurity trends: however, there needs to be a bigger spotlight on the good that hackers can do to protect the personal security of Americans in their daily lives and the confidential information exchanged in the business community. The more awareness about cybersecurity and good hackers (also known as information security researchers), the more protected U.S. businesses and citizens will be from cyberattacks.

While businesses are taking security measures to help assure their customers are making safe online purchases, there is no guarantee. Responsibility of security is a two-way street between businesses or, in the case of this survey, retailers and consumers. Although the majority of Americans surveyed said that retailers hold the responsibility, younger Americans feel a responsibility to protect their data. As retailers can only do so much, all Americans, regardless of age, need to take security into their own hands - starting with learning basic security best practices to protect themselves online and using an internet security solution on all of their personal devices.

One of the keys to internet security is preventing an attack before it happens. For example, ransomware is a growing epidemic around the world, which has significantly impacted consumers and businesses. Once infected, it is almost always too late for the victim. Given this rising threat as well as others, it's also critical to understand your employer's cybersecurity policies and to protect your personal information while at work.

From a business perspective, the most important type of data Americans expect a company to pay to get back if they become the victim of a ransomware attack is employee social security numbers, followed by customer banking details and employee banking details. These findings provide a clear understanding that safeguarding personally identifiable information (PII) is a top priority to U.S. adults, whether they are the customer or the employee of the affected business.

Ensuring businesses and consumers have an understanding of security and how to protect themselves online is crucial for protecting our digital society. As the threat landscape continues to evolve, Americans using the internet, whether while at home or at work, should learn about the indicators of cyberthreats and follow the proper steps to proactively protect themselves and the economy.

Kaspersky Lab and HackerOne are committed to informing consumers and businesses of the latest cyberthreats they may face and the best approaches for safeguarding their personal and company information.

About HackerOne

HackerOne is the #1 bug bounty platform, connecting organizations with the world's largest community of highly-qualified hackers. More than 700 organizations, including The U.S. Department of Defense, General Motors, Uber, Twitter, GitHub, Nintendo, Starbucks, Square, Dropbox and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities before criminals can exploit them. HackerOne customers have resolved more than 37,000 vulnerabilities and awarded more than $13,000,000 in bug bounties. HackerOne is headquartered in San Francisco. For more information, please visit https://hackerone.com.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into 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 Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

i. HackerOne's 2016 Bug Bounty Hacker Report
ii. Business Insider article "Inviting the hacker in"
iii. HackerOne Bug Bounty Program Definition
iv. Kaspersky Lab's Corporate IT Security Risks Report 2016
v. Kaspersky Security Bulletin 2016 – Story of the Year: The Ransomware Revolution
vi. FBI ransomware definition
vii. Kaspersky Lab Ransomware Report 2016