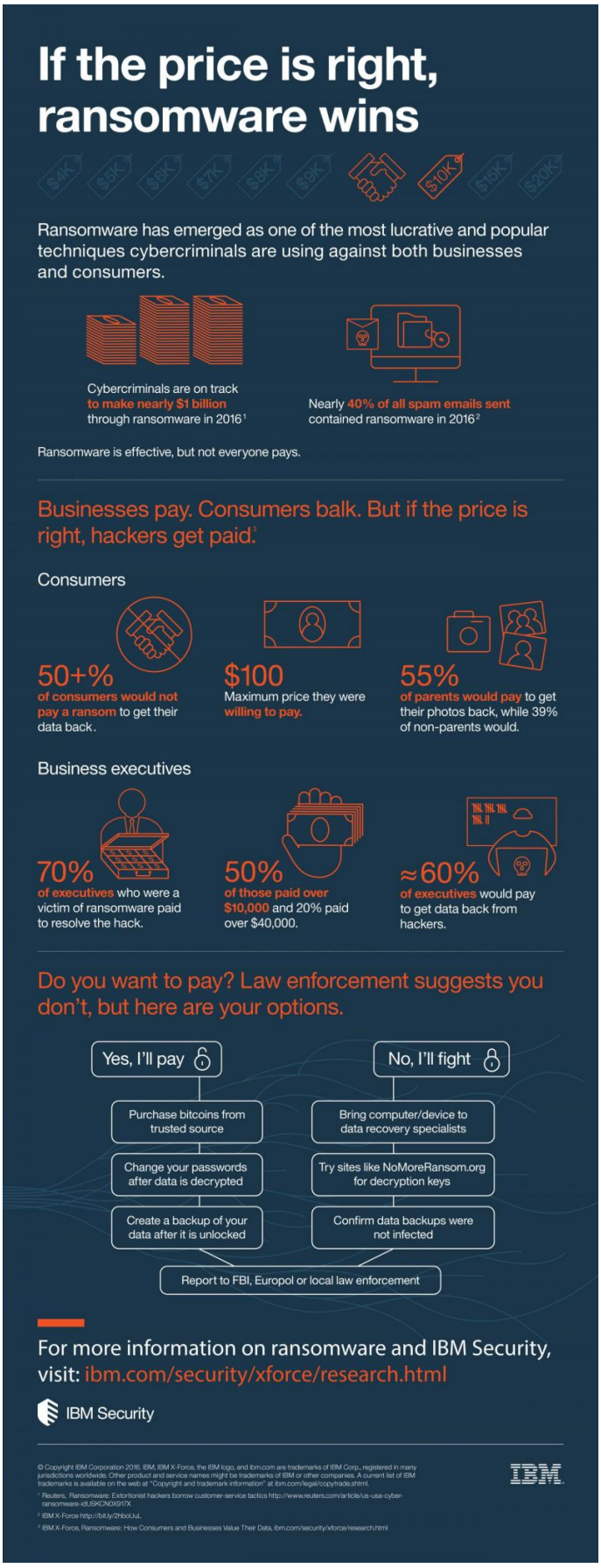
Businesses more likely to pay ransomware than consumers, study says

December 15 2016, by Kelly Kane


If the price is right, ransomware wins
$4K
$5K
$6K
$7K
$8K
$9K
$10K
$15K
$20K
Ransomware has emerged as one of the most lucrative and popular techniques cybercriminals are using against both businesses and consumers.
Cybercriminals are on track to make nearly $1 billion through ransomware in 2016[1]
Nearly 40% of all spam emails sent contained ransomware in 2016[2]
Ransomware is effective, but not everyone pays.
Businesses pay. Consumers balk. But if the price is right, hackers get paid.[3]
Consumers
50+%
of consumers would not pay a ransom to get their data back.
$100
Maximum price they were willing to pay.
55%
of parents would pay to get their photos back, while 39% of non-parents would.
Business executives
70%
of executives who were a victim of ransomware paid to resolve the hack.
50%
of those paid over $10,000 and 20% paid over $40,000.
≈60%
of executives would pay to get data back from hackers.
Do you want to pay? Law enforcement suggests you don't, but here are your options.
Yes, I'll pay
Purchase bitcoins from trusted source
Change your passwords after data is decrypted
Create a backup of your data after it is unlocked
No, I'll fight
Bring computer/device to data recovery specialists
Try sites like NoMoreRansom.org for decryption keys
Confirm data backups were not infected
Report to FBI, Europol or local law enforcement
For more information on ransomware and IBM Security, visit: ibm.com/security/xforce/research.html
IBM Security
© Copyright IBM Corporation 2016. IBM, IBM X-Force, the IBM logo, and ibm.com are trademarks of IBM Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml.
[1] Reuters, Ransomware: Extortionist hackers borrow customer-service tactics http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X
[2] IBM X-Force http://bit.ly/2hboUuL
[3] IBM X-Force, Ransomware: How Consumers and Businesses Value Their Data, ibm.com/security/xforce/research.html
IBM

Credit: IBM

IBM Security today announced results from a study finding 70 percent of businesses infected with ransomware have paid ransom to regain access to business data and systems. In comparison, over 50 percent of consumers surveyed said they would not pay to regain access back to personal data or devices aside from financial data.

Ransomware is an extortion technique used by cybercriminals where data on computers and other devices is encrypted and held for ransom until a specified amount of money is paid. The IBM X-Force study, "Ransomware: How Consumers and Businesses Value Their Data" surveyed 600 business leaders and more than 1,000 consumers in the U.S. to determine the value placed on different types of data. Some key findings from consumers include:

- While over half of consumers surveyed initially indicated they would not pay the ransom, when asked about specific data types, 54 percent indicated they would likely pay to get financial data back.
- Also, more than half (55%) of parents surveyed would be willing to pay for access to digital family photos vs. 39 percent of respondents without children.

Ransomware was one of the leading cybersecurity threats in 2016 with the FBI estimating cybercriminals, in the first three months of this year, making a reported $209 million. This would put criminals on pace to make nearly $1 billion in 2016 from their use of the malware. In fact, according to IBM X-Force research, ransomware made up nearly 40

percent of all spam e-mails sent in 2016, demonstrating a significant increase in the spread of the extortion tool.

Businesses Paying Up

Demonstrating ransomware's success with businesses, nearly one in two business executives surveyed have experienced ransomware attacks in the workplace. The study found 70 percent of these executives said their company has paid to resolve the attack, with half of those paying over $10,000 and 20 percent paying over $40,000.

As part of the survey, nearly 60 percent of all business executives indicated they would be willing to pay ransom to recover data. The data types they were willing to pay for included financial records, customer records, intellectual property and business plans. Overall, 25 percent of business executives said, depending upon the data type, they would be willing to pay between $20,000 and $50,000 to get access back to data.

Small businesses remain a ripe target for ransomware. Only 29 percent of small businesses surveyed have experience with ransomware attacks compared to 57 percent of medium size businesses. While cybercriminals may not view these businesses as offering a big payday, a lack of training on workplace IT security best practices can make them vulnerable. The study found that only 30 percent of small businesses surveyed offer security training to their employees, compared to 58 percent of larger companies.

Consumers Can be Motivated to Pay

One out of two consumers participating in the survey indicated they would be unwilling to pay a hacker to regain access to their data. When presented with specific data types their willingness to pay began to

increase.

For example, 54 percent of participants would be willing to pay for financial data and 43 percent were willing to pay for access back to their mobile device. When asked to put a value on different types of data, 37 percent of consumers said they would pay over $100 to get data back. For comparison, IBM X-Force typically sees ransomware demanding approximately $500 or higher, depending upon the victim and the time lapse they wait before paying.

Cybercriminals are having their best success leveraging ransomware against parents. In fact, 39 percent of parents surveyed have experience dealing with ransomware while overall 29 percent of non-parents indicated some experience.

IBM's analysis determined that parents are more motivated to pay due to sentimental value and children's happiness. For example, 71 percent of parents surveyed were most concerned about their family digital photos and videos being threatened with only 54 percent of non-parents showing the same concern. Overall, 55 percent of parents would pay for access back to the photos while only 39 percent of non-parents would pay.

Access to gaming devices, likely used by children, were also highly ranked by parents as most concerning to them. In fact, it was second to photos and video with 40 percent of parents reported being worried about losing access to these devices versus 27 percent of non-parents.

"While consumers and businesses have different experiences with ransomware, cybercriminals have no boundaries when it comes to their targets," said Limor Kessem, Executive Security Advisor, IBM Security and the report's author. "The digitization of memories, financial information and trade secrets require a renewed vigilance to protect it from extortion schemes like ransomware. Cybercriminals are taking

advantage of our reliance on devices and digital data creating pressure points that test our willingness to lose precious memories or financial security."

Preparing for and Responding to Ransomware

With the financial returns on ransomware growing north of a $1 billion for cybercriminals, IBM anticipates it and other extortion schemes will continue to grow. Both businesses and consumers can take some steps to help defend themselves from ransomware. IBM X-Force experts recommends the following tips to protect yourself and your business:

- Be Vigilant: If an email looks too good to be true, it probably is. Be cautious when opening attachments and clicking links.
- Backup Your Data: Plan and maintain regular backup routines. Ensure that backups are secure, and not constantly connected or mapped to the live network. Test your backups regularly to verify their integrity and usability in case of emergency.
- Disable Macros: Document macros have been a common infection vector for ransomware in 2016. Macros from email and documents should be disabled by default to avoid infection.
- Patch and Purge: Maintain regular software updates for all devices, including operating systems and apps. Update any software you use often and delete applications you rarely access.

More information: For additional tips and details on the survey findings, you can download the full report at: ibm.biz/RansomwareReport

Provided by IBM