IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks

Majority Not Willing to Pay Higher Taxes to Protect Local Resources, 63% Prefer Paying Higher Repair Cost Over Using Tax Dollars for Ransom

CAMBRIDGE, Mass., Sept. 5, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security announced results of a new study that explores taxpayers' point-of-view on ransomware in the wake of growing attacks against cities. The survey, conducted by Morning Consult on behalf of IBM, highlights that nearly 80% of citizens surveyed across the United States are increasingly worried about ransomware attacks on cities - yet more than half are still hesitant to have city governments put forth the funds to fight off hackers or implement cybersecurity defenses to help protect against attacks in the first place.

The study findings explore the extent to which U.S. citizens understand the severity of ransomware attacks, what they're willing to contribute from their tax dollars, how they feel government leaders are handling the issue, and how they prioritize the services that are being targeted during attacks. With the FBI reporting nearly 1,500 ransomware attacks in 2018 alone, and more than 50 cities and government entities impacted by ransomware attacks in 2019 so far, preparation for these threats remains critical. The results illustrate a divide between surveyed taxpayer's expectations and public official's resources, creating a challenge for local and state governments combating and managing the threat of ransomware.

Sponsored by IBM Security and conducted by Morning Consult, the study was compiled based on the responses of 2,200 US citizens spanning various city sizes, ages, incomes, political views, and more. Key findings from the study include:

- **Ransomware Hits Home:** Taxpayers see ransomware as a threat to their personal data and their city's data**.** 75% of respondents expressed concern around ransomware threats to their personal data, while nearly 80% fear ransomware's impact on cities across the U.S.
- **Taxpayers Say Don't Pay Ransom:** Nearly 60% of U.S. citizens surveyed are against their local governments using tax dollars to pay ransoms
- **Wait and See Attitude:** Taxpayers would rather see ransomware play out than pay up**.** More than 60% of respondents would prefer their city to deal with the larger recovery costs rather than use tax dollars to pay ransom in a ransomware attack
- **Who is Responsible?:** Just under half of responding citizens believe protecting cities from ransomware is the federal government's job, above state and local decision makers - and nearly 90% of U.S. citizens are in favor of increasing federal funding to improve cybersecurity in cities

"The use of ransomware to hold cities hostage for ransom payments continues to grow, and as those impacted pay off the attackers' ransom, the more the price continues to increase," said Wendi Whitmore, Vice President X-Force Threat Intelligence, IBM Security. "One common misconception is that paying the ransom immediately solves the problem, however doing so doesn't always guarantee swift recovery of infected devices. It requires significant time and investment to decrypt devices, and there's always the chance that paying criminals still won't result in unlocked files at all."

What Government Services and Systems Do Taxpayers Prioritize?

While citizens are most likely to support payment of ransoms for services they see as critical, the services they do not consider critical are surprising. More than 30% of taxpayers surveyed wouldn't support payment of any

amount to assist 911 emergency services, police departments, and school systems if they were targeted by a cyberattack. Even those who were willing to pay to restore critical emergency services were, in many cases, often only willing to do so if the cost ran below $50,000. Nearly 40% of respondents specifically noted they wouldn't pay anything to assist K-12 public schools or police departments.

Role of Government in Responding to Ransomware

According to a 2018 survey of state Chief Information Security Officers, "nearly half of all U.S. states do not have a cybersecurity budget line item," and "more than a third have seen no growth or a reduction in those budgets. State enterprise IT budgets allocated to enterprise cybersecurity is 1–2 percent, and annual budget increases have not kept pace with the needs of today's security landscape and tomorrow's evolving challenges."[1]

The IBM survey found that U.S. citizens seem to be looking to the federal government for leadership when it comes to handling the issue of ransomware. While attacks are primarily being seen at the local government level, almost half of respondents consider ransomware to be the federal government's job.

Additionally, citizens are much more willing to see the federal government pay to implement better cybersecurity, rather than pulling from their own local tax dollars - nearly 90% of taxpayers surveyed are in favor of increasing federal funding for local governments to improve cybersecurity. And for those who have already been hit by these attacks, more than three-quarters of responding citizens believe the federal government should be reimbursing those cities who continue to be crippled by the aftermath of their attacks.

Preparing for and Managing Ransomware Attacks

IBM X-Force Incident Response and Intelligence Services (IRIS) offers the following recommendations for organizations, cities, government entities, and beyond on how they can prepare for ransomware attacks:

- **Rehearse and Test Your Incident Response:** It's not a matter of *if* an incident response plan will be tested anymore, but a matter of *when*. Create a detailed incident response plan and conduct regular simulations with your stakeholders to test your response.
- **Maintain Backups, Test Backups, And Keep Offline Backups:** Backing up systems is a critical best practice. Ensuring departments have effective backups of critical systems *and are testing these backups* is more important than ever. Store backups apart from your primary network and only allow read, not write, access to the backups. Offline backups are ideal for the most sensitive data and systems.
- **Develop an Action Plan for Quickly Establishing Temporary Functionality:** Consider developing a capability to set up a short-term, quick turnaround business function to enable continued operations while an attack is being remediated. Create an alternative location and network for functions to continue critical services and systems in the face of attacks, even as remediation of or replacement of the original network is ongoing.
- **Patch Systems:** Ensure all systems are patched with the latest software updates.
- **Empower Employees:** Some of the best responses to cyberattacks can stem from empowered employees that are allowed to take calculated risks to save digital assets.
- **Hire an Ethical Hacker:** Departments should constantly test their security measures, including testing employees to identify weaknesses. Learn your group's risk level by having a hacker hack your department before a criminal does.

To download the full report of the survey results, go to http://ibm.biz/survey-cities

For more information on IBM X-Force IRIS go to http://ibm.biz/IBM-X-Force-IRIS. If you're experiencing an

emergency, contact IBM X-Force IRIS' incident response 24/7 hotline: 888-241-9812

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contacts:

Kim Samra
IBM Security Media Relations
ksamra@ibm.com
510-468-6406

[1] Deloitte and NASCIO, *2018 Deloitte-NASCIO Cybersecurity Study – States at risk: Bold plays for change*, (2018), 7-19

SOURCE IBM