IBM Newsroom

IBM Survey: Only 38% of State and Local Government Employees Trained on Ransomware Prevention

Two thirds of government employees surveyed concerned about cyberattacks on their workplace, threats against elections among top concerns in 2020

CAMBRIDGE, Mass., Feb. 27, 2020 /PRNewswire/ -- IBM (NYSE: IBM) Security today released the results of a new poll of U.S. city and state employees which examines their preparedness for dealing with cyberattacks. The study found that 73% of government employees surveyed are concerned about impending ransomware threats to cities across the country, and more employees fear of cyberattacks to their community than natural disasters and terrorist attacks.

More than 100 cities across the United States were hit with ransomware in 2019, according to research from Emsisoft. Data in the new Harris Poll, sponsored by IBM Security, found ransomware attacks might be even more widespread, with 1 in 6 respondents disclosing their department was impacted by a ransomware attack. Despite the growth of these attacks, half of the employees surveyed have not seen any change in preparedness from their employers, with only 38% receiving general ransomware prevention training. Also, budgets for managing cyberattacks have remained stagnant according to 52% of state and local government IT/Security professionals polled.

"The emerging ransomware epidemic in our cities highlights the need for cities to better prepare for cyberattacks just as frequently as they prepare for natural disasters," said Wendi Whitmore, VP of Threat Intelligence, IBM Security. "The data in this new study suggests local and state employees recognize the threat but demonstrate over confidence in their ability to react to and manage it. Meanwhile, cities and states across the country remain a ripe target for cybercriminals."

2020 Elections Concerns

With the impending 2020 election in the U.S, it's no surprise election security is top of mind for government employees. In fact, the new IBM Harris Poll study found 63% of respondents are concerned that a cyberattack could disrupt the upcoming elections, with the majority of government employees placing their local Board of Elections among the top three most vulnerable systems in their communities.

While concerns of attacks against election systems and voting machines continue to make headlines, cyberattacks can also be used as a form of distraction or a way to weaken confidence in systems for voters, or even impede them from casting ballots. The Cybersecurity Infrastructure Security Agency (CISA) has warned that ransomware attacks, in particular, pose a heightened risk to the elections. According to the study, the fear of ransomware attacks feels real to the vast majority of responding government employees, with 73% expressing concerns about threats to U.S. cities.

Public Education

Public schools have emerged as a growing target for cybercriminals in 2019, ranking as the 7th most targeted industry according to IBM's X-Force Threat Intelligence Index (moving up from 9th the year prior). Ransomware impacted school districts in New York, Massachusetts, New Jersey, Louisiana and other states last year.

The IBM Harris Poll study found that education respondents had the lowest amount of cybersecurity training compared to other surveyed state and local professionals. In general, 44% of those from the public education sector said they hadn't received basic cybersecurity training, and 70% said they hadn't received adequate training specifically on how to respond to a cyberattack. With low training numbers, the majority of education respondents aren't overly confident in their ability to recognize and prevent a ransomware attack – confidence is nearly 20% lower than other state and local employees surveyed.

Calling on the Federal Government

With ransomware attacks against cities likely to continue in 2020, both U.S. government employees and taxpayers believe the federal government should step in to assist. The survey shows 78% of government employees believe the federal government should provide assistance to communities in responding to cyberattacks, echoing sentiments from IBM's 2019 study where 50% of U.S. taxpayers said it's the federal government's responsibility to protect cities from ransomware. The majority (76%) of state and local employees also believe cyberattacks warrant emergency support, similar to those used for natural disasters.

Positive Progress and the Path Forward for Cities

While the study details where work needs to be done in preparing cities for cyberattacks, the results also showed some improvements made since last year. When asked whether they had seen any increases in preparedness and concern for cybersecurity in their departments, government employees surveyed claimed they had seen more improvements than not, and nearly 70% think their employers are currently taking the threat of cyberattacks seriously. City and state employees ranked ransomware #3 among the threats they were most familiar with – demonstrating that well publicized attacks are increasing awareness.

To expand on these improvements, IBM Security is encouraging U.S. cities to strengthen their preparedness through collaboration and threat sharing, creating and implementing incident response plans, and regularly testing their preparedness via threat simulations. IBM X-Force IRIS has been closely working with dozens of city experts and law enforcement agencies to encourage local governments across the U.S. to get a jump start on their cybersecurity preparedness and become better equipped to handle impending threats.

To download the full report of the survey results, go to ibm.biz/city-employees

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 the Survey & IBM Security Ransomware Research

This survey was conducted online by The Harris Poll on behalf of IBM among 690 employees who work for state or local government organizations in the United States. The survey was conducted January 16 through February 3, 2020 among adults 18+, employed full time or part time by local or state government. Four groups were captured in this survey:

1. Local and state employees (working across all public sectors)
2. Local and state employees in IT & related activities
3. Local and state employees in public safety/emergency response
4. Local and state employees in public education

Each group was weighted to their respective population by education, age, gender, race, Hispanic ethnicity, US region, household income, full-time/part-time employment status and local/state level to population benchmarks from the March 2019 Current Population Survey (CPS), conducted by the US Census Bureau. For all groups, propensity score weighting was also used to adjust for respondents' propensity to be online.

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.

Contact: Kimberly Samra, IBM Security, (510) 468-6406, ksamra@ibm.com

SOURCE IBM

Additional assets available online: 

https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention