ICMA | survey research

LOCAL GOVERNMENT CYBERSECURITY PRACTICES

In 2016, the International City/County Management Association (ICMA), in partnership with the University of Maryland, Baltimore County (UMBC), conducted a survey to better understand local government cybersecurity practices. The results of this survey provide insights into the cybersecurity issues faced by U.S. local governments, including what their capacities are, what kind of barriers they face, and what type of support they have to implement cybersecurity programs.

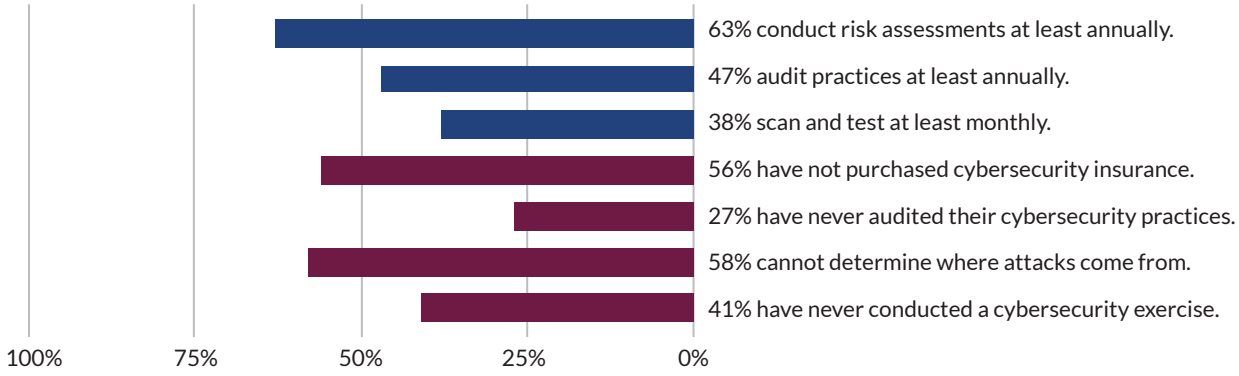
Since these survey results were released in April 2017, high-profile cyberattacks impacting transit, utility, and financial systems in places like **Sweden, Sacramento, Baltimore,** and **Atlanta** have heightened interest in these findings.

Local governments of all sizes and locations now own and operate a wide and growing array of internet-connected technology systems: employee-issued laptops, motion sensors on light poles and under pavement, mapping and informational systems inside police cars, online citizen-engagement tools and much more.

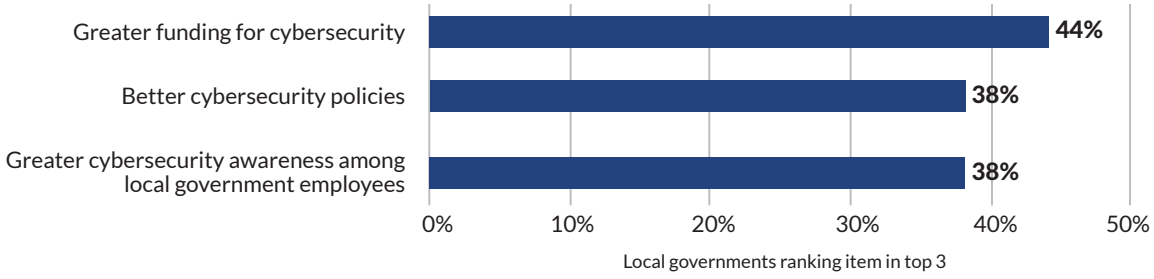
Most local governments in the United States don't have a strong grasp of the policies and procedures they should implement to protect their technology systems from attacks.

— ICMA op-ed, The New York Times, March 30, 2018

Approximately 1 in 3 local governments **don't know** how frequently their information system is subject to **attacks, incidents,** and **breaches**. Of those that do, **60%** report they are subject to **daily cyberattacks,** often hourly or more.



Top 3 things that local governments need most to ensure the highest level of cybersecurity (n=323)



Even when local governments do have top-notch cybersecurity, [Emeritus Prof. Donald Norris from UMBC] said, one mistake by one employee — opening a malicious email, leaving a port open — can open the door to an attack.

Cory Fleming [from ICMA] said government workers need better training and stronger cybersecurity policies to protect against attacks.

— The Baltimore Sun, March 29, 2018

Local government managers are best equipped to lead their organizations towards cybersecurity best practice. When cybersecurity professionals rated members of their local government for cybersecurity awareness:

62%
rated managers as at least moderately aware

26%
rated council members as at least moderately aware

34%
rated the average end user (i.e., local government staff) as at least moderately aware

We must actively prepare for cyberthreats of the sort that have been demonstrated in places like Atlanta. We don't need to halt technological deployments and evolution, but we do need to recognize that cybersecurity is an essential counterpart.

— ICMA op-ed, The New York Times, March 30, 2018

Resources

- A detailed introduction to cybersecurity by the Department of Homeland Security: www.dhs.gov/topic/cybersecurity
- An overview of risk management by the National Institute of Standards and Technology: csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
- ICMA-Microsoft Cybersecurity Report: www.icma.org/cyber-report
- ICMA Cybersecurity Survey Report: www.icma.org/documents/icma-survey-research-cybersecurity-2016-survey
- How to develop a city strategy for cybersecurity by Microsoft: www.microsoft.com/en-us/cybersecurity/content-hub/developing-city-strategy-for-cybersecurity
- Dekalb County, GA Information Technology Strategic Plan: www.dekalbcountyga.gov/information-technology/welcome
- California Department of Technology Information Security page including resources on policies, oversight, operations: www.cdt.ca.gov/security

For additional information, please contact ICMA survey research at surveyresearch@icma.org.