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.


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.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>63%</td>
<td>Conduction risk assessments at least annually.</td>
</tr>
<tr>
<td>47%</td>
<td>Audit practices at least annually.</td>
</tr>
<tr>
<td>38%</td>
<td>Scan and test at least monthly.</td>
</tr>
<tr>
<td>56%</td>
<td>Have not purchased cybersecurity insurance.</td>
</tr>
<tr>
<td>27%</td>
<td>Have never audited their cybersecurity practices.</td>
</tr>
<tr>
<td>58%</td>
<td>Cannot determine where attacks come from.</td>
</tr>
<tr>
<td>41%</td>
<td>Have never conducted a cybersecurity exercise.</td>
</tr>
</tbody>
</table>

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

- Greater funding for cybersecurity (44%)
- Better cybersecurity policies (38%)
- Greater cybersecurity awareness among local government employees (38%)
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.


### Resources

- Dekalb County, GA Information Technology Strategic Plan: [www.dekalbcountyga.gov/information-technology/welcome](http://www.dekalbcountyga.gov/information-technology/welcome)
- California Department of Technology Information Security page including resources on policies, oversight, operations: [www.cdt.ca.gov/security](http://www.cdt.ca.gov/security)

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