Securing The Perimeters

A Candid Survey on Cybersecurity in State and Local Governments
Table of Contents

—
Overview / 3

—
Executive Summary / 5

—
Research Findings / 6

—
Final Considerations / 16

—
Respondent Profile / 17

—
About / 19
Overview

Purpose

State and local governments face a multitude of cybersecurity threats unique to their regional and municipal oversight. Unlike their federal agency counterparts, in many cases these departments lack the centralized resources, strategy, and financial backing necessary for investing in a strong, agile cybersecurity workforce. It is critical for state and local leaders to maximize the resources they do have in order to weather the most damaging attacks from fraudsters, hacktivists, and common criminals seeking to steal sensitive information or access critical controls.

Methodology

To assess the perceptions, attitudes, and experiences that state and local leaders have regarding cybersecurity in their respective government sectors, GBC and CenturyLink deployed a survey to a random sample of state and local online subscribers of Government Executive and Route Fifty in July 2016. At least 328 state and local government leaders from across 43 states completed the survey, 62% of whom identify as VP/senior level or above. Respondents include representatives from at least 26 mission areas, with 77% reporting they oversee at least one direct report.
Given the motivations and capabilities of those who seek to damage the United States, the increasingly accessible means for committing cyber crime and the difficulty of thwarting attacks with hidden attribution, we need to recognize that there will likely be a utility cyber disruption at some point. And given the extent to which both our quality of life and sheer survival depend upon modern utilities, the nascent area of recovery management deserves serious, urgent attention.

Executive Summary

Cybersecurity is high priority, but limited resources hinder progress

Most respondents agree their government’s leaders consider cybersecurity a high priority. Even so, respondents consistently indicate that the most valuable resources to ensuring strong cybersecurity are either in low supply at their agency or out of reach. Lack of in-house cyber personnel, low cyber awareness in the workforce, and budget constraints emerge as some of the most formidable roadblocks to agencies pushing for improved cybersecurity.

Lack of cyber personnel contributes to feelings of vulnerability

Fewer than 1 in 2 respondents agree that their organization has the in-house expertise necessary to defend against the latest cyber threats. Moreover, 39% of respondents also feel that state and local government agencies are more vulnerable to cyber threats than their federal counterparts. Not only are organizations in need of skilled talent, but in many cases they lack the analytics to aid cyber professionals while on the job. For example, 55% of respondents do not know if their organization leverages analytics to improve detection.

Respondents see cyber awareness as major area for improvement

47% of respondents describe the depth of cyber awareness training they’ve received as basic training (i.e., provided via company-provided policy manuals or emails). And more than a fifth report having received no cybersecurity training at all. Despite many saying that increased employee awareness (46%) was a top priority in the past year, 55% still believe escalating such awareness efforts, in tandem with greater investment in cyber technologies, will enact the most positive effect on their agency’s cybersecurity posture going forward.

Most fear cyberthreats will adversely impact privacy, data integrity

47% of respondents are very concerned about their ability to prevent cyberthreats targeting privacy, with data integrity (42%) and public safety (36%) also high on the list of concerns. In this context, it makes sense that fraud perpetrators (61%) and hacktivists (59%) should emerge as the top threats because of the damage they can wreak on both privacy and data integrity. By comparison, the next most severe threat is perceived to be the one from within—the insider threat, at 33%. Clearly, respondents are weary that the most damaging enemies are the ones disguised as innocuous parties or invisible altogether.
Research Findings

Overall, state and local leaders are generally confident in their government’s cybersecurity stance:

- "Compared to other objectives, cybersecurity is considered a high priority for leaders in the government in which I serve."

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>48%</td>
<td>17%</td>
<td>3%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Percentage of respondents, n=304
Note: Percentages may not add up to 100% due to rounding

- "I believe my organization has the in-house expertise needed to effectively defend against the latest cyber threats."

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>6%</td>
<td>41%</td>
<td>29%</td>
<td>12%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Percentage of respondents, n=259
Note: Percentages may not add up to 100% due to rounding

77% of respondents agree or strongly agree that their government considers cybersecurity a high priority when compared to other mission objectives.

However, despite general agreement as to cybersecurity’s high priority, respondents are more reserved in their assessments of current cyber personnel readiness.

Whereas 47% agree or strongly agree their government has the in-house expertise needed to effectively defend against the latest cyberthreats, another 41% disagree or strongly disagree with the claim, an indication that more can be done to fill the current skills gap at the state and local level.
Many respondents view their agencies as more vulnerable to cyberthreats than federal agencies / Research Findings

39% of respondents believe state and local governments are more vulnerable to cyberthreats than their counterparts in the federal sector, and many attribute this to constraints on cybersecurity spending and a shortage of in-house cyber personnel.

---

In your opinion, are state and local governments more or less vulnerable than federal government agencies to cyberthreats?

- Much more vulnerable: 7%
- More vulnerable: 32%
- Equally vulnerable: 40%
- Less vulnerable: 12%
- Much less vulnerable: 0.3%
- Don't know: 9%

---

Among respondents who say “more vulnerable”:

Why do you think this might be? Please select all that apply.

- Budget constraints limit ability to spend on cybersecurity: 67%
- Shortage of in-house cyber personnel: 59%
- Potentially seen as easier target than federal agencies: 50%
- Lack of unified cyber policies across states and localities: 41%
- Limited ability to share cost of large-scale technology implementations: 40%
- Lack of collaboration/information sharing among states and localities: 37%
- Increased risk to public safety because of state/local oversight of utilities/critical infrastructure: 20%
- Other: 2%

Percentage of all respondents, n=305
Note: Percentages may not add up to 100% due to rounding

Percentage of respondents, n=119
Respondents were asked to select all that apply
Respondents are most concerned cyberthreats will negatively impact privacy and data integrity / Research Findings

Privacy gives respondents the most anxiety when considering the potential impact of cyberthreats on an organization’s infrastructure, with 47% saying they are very concerned in their government’s ability to handle this sort of an attack. Though not as concerning as attacks impacting privacy, other threats targeting data integrity (42%) and public safety (36%) cause trepidation as well.

<table>
<thead>
<tr>
<th>Category</th>
<th>Not concerned</th>
<th>Somewhat concerned</th>
<th>Very concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy (e.g., access to citizen data, personally identifiable information)</td>
<td>8%</td>
<td>45%</td>
<td>47%</td>
</tr>
<tr>
<td>Data Integrity (e.g., loss or destruction of data or information)</td>
<td>8%</td>
<td>50%</td>
<td>42%</td>
</tr>
<tr>
<td>Public Safety (e.g., attacks on critical infrastructure, safety services)</td>
<td>11%</td>
<td>53%</td>
<td>36%</td>
</tr>
<tr>
<td>Proprietary Data (e.g., confidential agency data or intellectual property)</td>
<td>14%</td>
<td>53%</td>
<td>33%</td>
</tr>
<tr>
<td>Availability of Services (e.g., disruptions to online or in-person government services)</td>
<td>16%</td>
<td>53%</td>
<td>31%</td>
</tr>
</tbody>
</table>

Note: Percentages may not add up to 100% due to rounding.
Respondents see fraud perpetrators and hacktivists as most pervasive threats to data security / Research Findings

**From your perspective, which of the following groups constitute the greatest threat to the security of your government’s data, information, or online services? Please select all that apply.**

<table>
<thead>
<tr>
<th>Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud perpetrators</td>
<td>61%</td>
</tr>
<tr>
<td>Hacktivist groups</td>
<td>59%</td>
</tr>
<tr>
<td>Employees within my organization (i.e., insider threats)</td>
<td>33%</td>
</tr>
<tr>
<td>Petty criminals</td>
<td>28%</td>
</tr>
<tr>
<td>Terrorist organizations</td>
<td>19%</td>
</tr>
<tr>
<td>Foreign government-sponsored actors</td>
<td>16%</td>
</tr>
<tr>
<td>Organized crime</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>None of the above</td>
<td>1%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>11%</td>
</tr>
</tbody>
</table>

In state and local governments, fraudsters and hacktivists present the greatest threats to an agency’s information and online services. The concern reserved for these two threats in particular is telling, as they exhibit a 28-pt. and 26-pt. spike respectively over the third most pressing threat, the one posed by employees within an organization (33%).

61% see fraud perpetrators as the greatest threat to their organization’s information security.
In past year, organizations most commonly sought to raise employee cyber awareness /

**Research Findings**

Among the steps organizations took to improve their cybersecurity over the past year, respondents most frequently cited efforts aimed at increasing general employee awareness and cyber hygiene (46%). Coinciding with this push toward education is a concerted step toward enhancing user access protocols and making sure users are assigned privileges that are appropriate to their job duties and station.

---

**Over the past year, what types of steps has your organization taken to improve its cybersecurity? Please select all that apply.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing employee awareness/cyber hygiene</td>
<td>46%</td>
</tr>
<tr>
<td>Enhancing user access protocols (e.g., password rules, user access requirements)</td>
<td>45%</td>
</tr>
<tr>
<td>Implementing more advanced cybersecurity technologies</td>
<td>34%</td>
</tr>
<tr>
<td>Tightening focus on cybersecurity basics (e.g., patching known vulnerabilities)</td>
<td>33%</td>
</tr>
<tr>
<td>Collaborating with departments/agencies within our government</td>
<td>25%</td>
</tr>
<tr>
<td>Working with managed security service providers</td>
<td>21%</td>
</tr>
<tr>
<td>Collaborating with departments/agencies in other governments (e.g., federal, state, local)</td>
<td>18%</td>
</tr>
<tr>
<td>Implementing multi-factor authentication</td>
<td>17%</td>
</tr>
<tr>
<td>Recruiting cyber personnel to improve in-house expertise</td>
<td>15%</td>
</tr>
<tr>
<td>Refining incident response planning and processes</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
<tr>
<td>None of the above</td>
<td>7%</td>
</tr>
<tr>
<td>Don't know</td>
<td>22%</td>
</tr>
</tbody>
</table>

"Other" includes responses such as enacting new state laws for educational institutions to protect student information, redesigning the agency website, working with a contract Data Processing Supplier, and purchasing cybersecurity insurance.
One reporting entity highlighted the importance of proactively establishing a working relationship with the technology department so that the lines of communication would be open if the entity needed assistance. Likewise, another reporting entity explained that its agency hosts bimonthly meetings for the information security officers from all the departments within its agency to promote sharing of issues, solutions, and best practices.

California State Auditor, High Risk Update – Information Security
Looking forward, cyber education and awareness still the top priority / Research Findings

Even though improving cyber awareness was at the top of last year’s agenda for most state and local respondents, that has not changed in strategizing for the year ahead. 55% still regard cyber hygiene as the leading difference maker in improving their organization’s cybersecurity posture, however greater investment in cyber technologies and cyber personnel are also highly regarded as potential game-changers.

---

In your opinion, which of the following changes would make the biggest difference in improving your organization’s cybersecurity posture? Please select all that apply.

<table>
<thead>
<tr>
<th>Change</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improving employee cyber awareness/cyber hygiene</td>
<td>55%</td>
</tr>
<tr>
<td>Greater investment in cyber technologies</td>
<td>41%</td>
</tr>
<tr>
<td>Greater investment in in-house cyber personnel</td>
<td>35%</td>
</tr>
<tr>
<td>Formally elevating cybersecurity to be an organizational strategic priority</td>
<td>31%</td>
</tr>
<tr>
<td>Increasing collaboration with other governments</td>
<td>24%</td>
</tr>
<tr>
<td>Establishing unified government cyber regulations statewide or nationwide</td>
<td>24%</td>
</tr>
<tr>
<td>Voiced support from state/local leaders</td>
<td>13%</td>
</tr>
<tr>
<td>Fostering better working relationships with managed security service providers</td>
<td>13%</td>
</tr>
<tr>
<td>Increasing the authority of my organization’s cyber decision makers</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>None of the above</td>
<td>0.4%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>18%</td>
</tr>
</tbody>
</table>

Percentage of respondents, n=259
Respondents were asked to select all that apply

With education, technology, and hiring cyber personnel receiving the brunt of attention, the data indicates that state and local government employees would like to devote more resources and funding to these three needs in particular, with more resource-independent approaches (e.g., voice support, increasing collaboration) taking a back seat.

55% of respondents believe improved cyber awareness and cyber hygiene will have the most positive impact on cyber readiness going forward.
Over half do not know if agency is using or plans to use analytics to thwart cyber attacks / Research Findings

55 percent of respondents are unaware if their organization uses or plans to use data analytics in order to improve detection and prevention of cyber attacks, reinforcing the point that improving employee awareness of cyber policies and cyberthreats will be a critical investment going forward. Moreover, 18%, or nearly 1 in 5 respondents, are positive their organization does not leverage nor plans to leverage analytics for improved cyber defenses.

What best describes your organization’s current plans for leveraging data analytics in order to improve detection and prevention of cyber attacks?

- Currently leveraging analytics: 15%
- Planning to leverage within the next 6 months: 4%
- Planning to leverage within the next 12 months or beyond: 8%
- Not planning to leverage: 18%
- Don’t know: 55%

Percentage of respondents, n=260
Note: Percentages may not add up to 100% due to rounding
Respondents express mixed feelings as to overall engagement of cybersecurity risks and training / Research Findings

In your opinion, how engaged are your organization’s employees when it comes to taking cybersecurity and cyber hygiene seriously?

- Very engaged: 7%
- Engaged: 24%
- Somewhat engaged: 30%
- Only a little engaged: 23%
- Not at all engaged: 8%
- Don’t know: 8%

Note: Percentages may not add up to 100% due to rounding

Only 31% of respondents view their organization’s employees as being engaged or very engaged when it comes to taking cybersecurity and cyber hygiene seriously.

Which of the following best describes the depth of cybersecurity awareness training you have received from your organization?

- Comprehensive, formal training (e.g., subject matter professionals, courses): 8%
- Basic, granular training (e.g., company-provided policy manuals/emails): 47%
- Informal instruction (e.g., from coworker or supervisor): 24%
- No instruction provided at all: 21%

Note: Percentages may not add up to 100% due to rounding

GBC asked respondents how they feel about the depth of cybersecurity awareness training they’ve received by their organizations. In response, 47% describe the extent of cyber awareness training they’ve received as basic, granular training, whether in the form of company-provided policy manuals or onboarding email tutorials. And more than a fifth of respondents report having received no cybersecurity training or instruction whatsoever.
Lawmakers don’t want to spend money on something that is **invisible**; they can’t visualize the damage, so they won’t fund what’s required... [They] need to see that this is a **critical** issue, which they need to embrace.

*Mark Weatherford, former Chief Information Security Officer, State of California*
Final Considerations

—

To alleviate resource gap, consider investing in analytics

Even if analytics require an upfront investment, it’s one that many experts say pays off in dividends later on. Given that state and local agencies face a shortage of cyber personnel, pursuing an aggressive analytics platform can go a long way in relieving that burden. In particular, analytics opens the door for automating various essential cyber practices, such as running internal diagnostic audits, monitoring user activity, detecting anomalous or suspicious material and alerting the appropriate authorities, as well as reducing duplicative procedures and redundancies in information maintenance. With only 15% of state and local respondents acknowledging the current use of analytics, this should be an increasing priority for many governments.

—

State and local government can expand, emphasize cyber education

Clearly, education and proper awareness of the full range of cyber threats is a recognized imperative by the majority of state and local respondents. While these findings show employees are, on the whole, somewhat engaged when it comes to cybersecurity matters, less than 10% reported receiving anything beyond a baseline level of instruction in cybersecurity best practices. State and local governments can seize this opportunity by initiating more comprehensive training across the board, enlisting employees in a number of different online courses during the onboarding process or by inviting a subject matter professional to expound on fundamental cybersecurity points. In any case, respondents agree awareness is critical. Now it’s up to state and local leaders to respond.
Respondent Profile

A majority of state and local respondents identify as leaders within their organization.

**Employment Situation**
- State government: 20%
- County or county equivalent government: 24%
- Municipal government: 50%
- Township government: 5%
- Independent school district government: 0.3%
- Independent special district government: 1%

**Role**
- C-suite/executive level: 38%
- VP/senior level: 25%
- Mid-level: 33%
- Entry/junior level: 5%

**Reports/oversees**
- 1 to 5: 27%
- 6 to 20: 17%
- 21 to 50: 15%
- 51 to 200: 11%
- Over 200: 7%
- None: 23%

80% of respondents hold positions in local government positions, whether at the county, municipal, township, or independent district levels.

63% of respondents identify as working at the VP/senior level or above.

77% of respondents are supervisors who oversee at least one employee, either directly or through direct reports.
Respondents represent over 43 states and at least 26 unique mission areas. Respondent Profile

Mission area
- Finance & Budget 10%
- Community Planning/Devel. 9%
- Police/Law Enforcement 7%
- Executive Offices 7%
- Healthcare & Human Services 6%
- Tax & Revenue 5%
- Legislative/Policy 4%
- Justice/Courts 4%
- Education 4%
- Fire/EMS 4%
- Transportation/Infrastructure 3%
- Energy & Utilities (Public Works) 3%
- Information Technology 3%
- Public Affairs/Communications 2%
- Housing & Urban Development 2%
- Corrections/Prisons 2%
- Social Services/Child Protection 2%
- Emergency Preparedness 1%
- Elections 1%
- Commerce 1%
- Aging 1%
- Waste Management 0.4%
- Libraries 0.4%
- Labor Relations 0.4%
- Environment & Natural Resources 0.4%
- Agriculture and Food 0.4%
- Other 18%

Percentage of respondents, n=247
Note: Percentages may not add up to 100% due to rounding

By Location
- Illinois
- North Carolina
- Texas
- Wisconsin
- California
- Missouri
- Georgia
- Ohio
- Pennsylvania
- Massachusetts
- New York
- Tennessee
- Connecticut
- Louisiana
- Michigan
- New Jersey
- Washington
- Arizona
- Indiana
- Maine
- Florida
- Minnesota
- Maryland
- Nebraska
- South Carolina
- Virginia
- Alabama
- Iowa
- Kansas
- Kentucky
- Mississippi
- Nevada
- New Mexico
- Oklahoma
- Rhode Island
- Utah
- West Virginia
- Wyoming
- District of Columbia
- Idaho
- New Hampshire
- Oregon
- Vermont

“Other” includes responses such as film and digital media office, codes enforcement and planning, and personnel administration.

States/jurisdictions are listed in order of frequency.
About

---

**Government Business Council**

As Government Executive Media Group’s research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive’s 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

**Report Author:** Daniel Thomas

---

**CenturyLink Government**

CenturyLink helps government, education and public safety sector organizations implement proven IT solutions to address public infrastructure continuity, ensure safety and security, facilitate economic growth, build stronger educational systems and augment technology needs. Our services are used by public sector customers of all sizes—from the largest and most critical government agencies to rural schools.

Learn more at [www.centurylink.com/GES](http://www.centurylink.com/GES)

---

**Contact**

**Will Colston**  
**Senior Vice President**  
**Strategic Marketing & Insights**  
**Government Executive Media Group**  
Tel: 202.266.7423  
Email: wcolston@govexec.com  
.govexec.com/insights  
@GovExecInsights