Bolstering the Pillars of IT

A Candid Survey of Government Officials on Agency IT Infrastructure
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Research Findings</td>
<td>4</td>
</tr>
<tr>
<td>Respondent Profile</td>
<td>18</td>
</tr>
<tr>
<td>About</td>
<td>20</td>
</tr>
</tbody>
</table>
Overview

Purpose

Government agencies provide crucial services and infrastructure to the American people, but how do their technologies fare in supporting mission-critical work? Are the IT systems secure? Are they current and able to meet today’s demands? To learn more, Microsoft and Lenovo surveyed government employees, particularly those supporting missions in the health and human services and transportation spheres of government.

Methodology

Between September and October of 2020, Microsoft and Lenovo issued a survey on IT infrastructure to federal and state and local government. 446 employees responded after quality control and screening, including 56% of respondents working in IT, procurement, and program management. 47% of respondents provide either health and human services or transportation and infrastructure services to their constituents. 60% of respondents are in federal government, while 40% are in state and local government.

For more information on respondents, please see the Respondent Profile.
Research Findings

Respondents have mixed feelings on whether their critical infrastructure relies on outdated technology

*To what extent do you agree or disagree with the following: "The critical infrastructure my agency supports is reliant on outdated technology."*

- **Strongly disagree**: 10%
- **Disagree**: 25%
- **Neither agree nor disagree**: 28%
- **Agree**: 27%
- **Strongly agree**: 10%

37% of respondents agree to some extent that their agency’s critical infrastructure relies on legacy architecture.

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

Over a third of respondents agree that their agencies continuously evaluate the cybersecurity of their critical infrastructure.

---

**To the best of your knowledge, about how often does your agency track cybersecurity progress of critical infrastructure?**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously</td>
<td>38%</td>
</tr>
<tr>
<td>Weekly</td>
<td>3%</td>
</tr>
<tr>
<td>Monthly</td>
<td>5%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>4%</td>
</tr>
<tr>
<td>Annually</td>
<td>2%</td>
</tr>
<tr>
<td>Never</td>
<td>3%</td>
</tr>
</tbody>
</table>

Percentage of respondents, n=343
Note: 45% of respondents "Not sure" is not shown above

17% of respondents think that their agencies less than continuously track cybersecurity progress of critical infrastructure.
As they age, legacy systems can be more costly to maintain, more exposed to cybersecurity risks, and less effective in meeting their intended purpose.

Research Findings

Most respondents are confident about inter-agency data in transit; however, some respondents remain skeptical.

How confident are you that critical data being transmitted between your organization and another agency is fully secure?

- Not at all confident: 7%
- Slightly confident: 14%
- Moderately confident: 43%
- Very confident: 31%
- Extremely confident: 6%

37% of respondents are very or extremely confident that critical data is being transmitted safely to other agencies.

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

Data sharing and analytics percolate to the top data challenges agencies face

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data analysis</td>
<td>46%</td>
</tr>
<tr>
<td>Inter-agency data sharing</td>
<td>40%</td>
</tr>
<tr>
<td>Intra-agency data sharing</td>
<td>40%</td>
</tr>
<tr>
<td>Using data on mobile laptops</td>
<td>29%</td>
</tr>
<tr>
<td>Securing data</td>
<td>25%</td>
</tr>
<tr>
<td>Using data at office workstations</td>
<td>19%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>

Of respondents, n=48
Note: Respondents were asked to select all that apply.

46% of respondents think that data analysis is amongst the top data challenges for their agency.
Please fill in the blank: "I am ________ required to submit dual-factor authentication whenever I access my work device(s)."

- 45% Always
- 17% Never
- 8% Rarely
- 16% Sometimes
- 14% Often

Percentage of respondents, n=331
Note: Percentages may not add up to 100% due to rounding.

25% of respondents rarely or never use dual-factor authentication whenever accessing their work devices.
How confident are you that your agency has each security component below to safeguard data of critical infrastructure?

- **Endpoint security**
  - Not at all confident: 4%
  - Slightly confident: 14%
  - Moderately confident: 27%
  - Very confident: 27%
  - Extremely confident: 29%

- **Network / WAN security**
  - Not at all confident: 6%
  - Slightly confident: 4%
  - Moderately confident: 35%
  - Very confident: 24%
  - Extremely confident: 31%

- **Zero trust data access security**
  - Not at all confident: 18%
  - Slightly confident: 18%
  - Moderately confident: 29%
  - Very confident: 24%
  - Extremely confident: 10%

- **Threat detection and remediation**
  - Not at all confident: 8%
  - Slightly confident: 16%
  - Moderately confident: 29%
  - Very confident: 31%
  - Extremely confident: 16%

Note: Percentages may not add up to 100% due to rounding.
**Research Findings**

Organizations’ cybersecurity tools and practices could be improved across the board

---

**How confident are you that your agency has each security component below to safeguard data of critical infrastructure?**

<table>
<thead>
<tr>
<th>Component</th>
<th>Not at all confident</th>
<th>Slightly confident</th>
<th>Moderately confident</th>
<th>Very confident</th>
<th>Extremely confident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal cybersecurity procedures and policies</td>
<td>8%</td>
<td>12%</td>
<td>35%</td>
<td>18%</td>
<td>27%</td>
</tr>
<tr>
<td>Formal cybersecurity education for all employees</td>
<td>10%</td>
<td>16%</td>
<td>22%</td>
<td>27%</td>
<td>24%</td>
</tr>
<tr>
<td>Firmware security</td>
<td>8%</td>
<td>13%</td>
<td>40%</td>
<td>25%</td>
<td>15%</td>
</tr>
<tr>
<td>Web-access security</td>
<td>6%</td>
<td>8%</td>
<td>29%</td>
<td>43%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Percentage of respondents, n=49

Note: Percentages may not add up to 100% due to rounding
Please rank the following in terms of current progress:

<table>
<thead>
<tr>
<th>Category</th>
<th>Not yet addressed</th>
<th>Plans in the making</th>
<th>Action plans implemented, but progress still needed</th>
<th>Progress being made</th>
<th>Fully implemented and modernized</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-office workstations</td>
<td>7%</td>
<td>2%</td>
<td>15%</td>
<td>24%</td>
<td>48%</td>
<td>4%</td>
</tr>
<tr>
<td>Cloud solutions to support analytics</td>
<td>9%</td>
<td>13%</td>
<td>20%</td>
<td>24%</td>
<td>17%</td>
<td>17%</td>
</tr>
<tr>
<td>Local hardware to support analytics</td>
<td>7%</td>
<td>11%</td>
<td>15%</td>
<td>22%</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Local hardware for network connectivity</td>
<td>9%</td>
<td>4%</td>
<td>15%</td>
<td>37%</td>
<td>24%</td>
<td>11%</td>
</tr>
<tr>
<td>IoT hardware</td>
<td>15%</td>
<td>17%</td>
<td>17%</td>
<td>13%</td>
<td>13%</td>
<td>24%</td>
</tr>
<tr>
<td>Mobile hardware</td>
<td>9%</td>
<td>4%</td>
<td>15%</td>
<td>28%</td>
<td>41%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Note: Percentages may not add up to 100% due to rounding.
We need to be more aggressive in determining what things can be done in a digital manner.

Suzette Kent, former Federal Chief Information Officer of the Trump Administration
"COVID-19 will ______ increase the number of people in my organization who work from home on a permanent basis."

- Not: 16%
- Mildly: 11%
- Moderately: 21%
- Very mildly: 9%
- Significantly: 43%

"My agency has supplied me with sufficient IT equipment to fulfill my work duties from home for the ______."

- Short term: 32%
- Long term: 43%
- My agency has not supplied me with sufficient IT equipment: 25%

25% of respondents say that their agencies have not provided them with sufficient IT equipment despite being over six months into the pandemic.
Microsoft has announced a new capability called Secured-core that allows companies to prevent attacks at the firmware level by establishing a secure root of trust that ensures that only valid software is allowed to execute upon boot.

How aware are you of this capability?

- Extremely aware: 4%
- Very aware: 6%
- Moderately aware: 13%
- Slightly aware: 13%
- Not at all aware: 64%

37% of respondents are aware of the Secured-core capability.
Which of the following have new specifications for purchasing equipment that require Secured-core PCs at your agency? Select all that apply.

- All new PC purchases: 31%
- Data analytics workstations: 22%
- Critical data access roles: 22%
- All mobile users: 20%
- Other: 6%

31% of respondents report that all new PC purchases must be Secured-core PCs, according to new specifications.

Percentage of respondents, n=54
Note: 44% of respondents selected “Don’t know.” Respondents were asked to select all that apply.
Research Findings

How valuable would it be for your agency to know that the BIOS and critical operating system software would be secure from the point of manufacture and continually updated while in use to protect from firmware-level attacks?

<table>
<thead>
<tr>
<th>Value</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all valuable</td>
<td>4%</td>
</tr>
<tr>
<td>Slightly valuable</td>
<td>4%</td>
</tr>
<tr>
<td>Moderately valuable</td>
<td>17%</td>
</tr>
<tr>
<td>Very valuable</td>
<td>30%</td>
</tr>
<tr>
<td>Extremely valuable</td>
<td>26%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>19%</td>
</tr>
</tbody>
</table>

56% of respondents think that this information would be very or extremely valuable to their agency.

Percentage of respondents, n=47
Note: 44% of respondents selected “Don’t know.” Respondents were asked to select all that apply.
Respondent Profile

A majority of respondents are federal government employees

60% Federal government
40% State and local

Over half of respondents work for the federal government.

Percentage of respondents, n=446
Note: Percentages may not add up to 100% due to rounding
Of the following, which service does your organization provide to its constituents?

- Health and human services: 20%
- Transportation and infrastructure: 27%
- Other: 53%

State and local government composition

- State government: 24%
- County or county equivalent government: 26%
- Municipal government: 42%
- Other independent regional district or authority: 3%
- Other: 5%

47% are involved with health and human services or transportation and infrastructure.
About Microsoft

At Microsoft, our mission is to empower every person and every organization on the planet to achieve more. Our mission is grounded in both the world in which we live and the future we strive to create. Today, we live in a mobile-first, cloud-first world, and the transformation we are driving across our businesses is designed to enable Microsoft and our customers to thrive in this world.

Learn more at www.Microsoft.com

About Lenovo

As the world’s #1 PC and tablet vendor, Lenovo is committed to providing secure technology and services for federal, state, and local government agencies. For more than 40 years, our customers have relied on us for reliable, high-performance devices and world-class support to meet their evolving needs.

To learn more, visit LenovoForGovernment.com