PRIMARY OBJECTIVES:

• Determine challenges faced by public sector IT professionals and sources of IT security threats
• Evaluate the importance of IT security products, solutions, and services and rate investment priorities
• Determine familiarity with the White House Cyber Security Executive Order and the perceived impact of its objectives
• Identify if organizations are using a zero-trust approach to IT, their motivations and deterrents, and evaluate the Principle of Least Privilege (PoLP)
• Measure the use of teleworking before COVID-19, currently, and in the future

Methodology

SolarWinds contracted Market Connections to design and conduct an online survey among 200 federal, 100 state and local, and 100 education decision-makers and influencers in October 2021. SolarWinds was not revealed as the survey sponsor.
Organizations Represented

All respondents work for the public sector with half in the federal government, one-quarter in state and local government, and one-quarter in education.

Which of the following best describes your current employer?
A range of state and local populations and school enrollments are represented in the sample. Smaller state, local, and education (SLED) populations and enrollments were excluded from participating.
Decision-Making Involvement

All respondents are knowledgeable or involved in decisions and recommendations regarding IT operations and management and IT security solutions and services.

- Develop technical requirements: 60%
- Evaluate or recommend firms: 52%
- On a team that makes decisions: 46%
- Manage or implement security/IT operations: 35%
- Make the final decision - technical aspects: 21%
- Make the final decision - financial aspects: 15%

Note: Multiple responses allowed

How are you involved in your organization’s decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)
Job Function and Tenure

A variety of job functions and tenures are represented in the sample, with most being IT staff and working at their current organization for 3-4 years, approximately half have a tenure of 3-14 years.

- **Job Function**
  - IT/IS staff: 47%
  - IT director/manager: 26%
  - Security/IA staff: 12%
  - Security/IA director or manager: 5%
  - CIO/CTO: 5%
  - CSO/CISO: 1%
  - Other: 5%

- **Tenure**
  - <1 Year: 12%
  - 1-2 Years: 9%
  - 3-4 Years: 13%
  - 5-9 Years: 16%
  - 10-14 Years: 20%
  - 15-19 Years: 18%
  - 20+ Years: 12%

Examples Include:
- Training
- Program manager
- Security research

Which of the following best describes your current job title/function? How long have you been working at your current organization?
Location of IT Security Products

IT security products are located primarily on-premises or in a private cloud. The respondents’ preferred location of these products is in some type of cloud, not on-premises. Federal respondents are more likely to prefer the private cloud.

<table>
<thead>
<tr>
<th>Currently located</th>
<th>Preferred location</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises/traditional data center</td>
<td>Federal</td>
</tr>
<tr>
<td>Government (private) cloud</td>
<td>62%</td>
</tr>
<tr>
<td>Public cloud</td>
<td>50%</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>15%</td>
</tr>
</tbody>
</table>

Note: Multiple responses allowed

Where are the IT security products your organization uses currently? Where would you prefer these products to be located? (select all that apply)

2019 Survey Data

- On-premises/traditional data center: Currently located 68%, Preferred location 57%
- Government (private) cloud: Currently located 50%, Preferred location 52%
- Public cloud: Currently located 19%, Preferred location 16%
- Hybrid cloud: Currently located 15%, Preferred location 18%

Note: Statistically significant difference

© 2021 Market Connections, Inc. © 2021 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED
IT Security Obstacles

Budget constraints top the list of significant obstacles to maintaining or improving organization IT security. Competing priorities and a complex internal environment also impact IT security improvement.

- Budget constraints: 30%
- Competing priorities and other initiatives: 15%
- Complexity of internal environment: 15%
- Lack of top-level direction and leadership: 12%
- Lack of manpower: 9%
- Inadequate internal collaboration with other teams: 8%
- Lack of technical solutions available at my organization: 5%
- Lack of training for personnel: 5%
- Lack of clear standards: 2%

What is the most significant high-level obstacle to maintaining or improving IT security at your organization?
IT Security Obstacles by Organization Type

- Education respondents cite lack of top-level direction and leadership as an obstacle more than other public sector respondents.

- State government respondents indicate more so than local governments that budget constraints are an obstacle to maintaining or improving IT security.

### Table: IT Security Obstacles by Organization Type

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Federal</th>
<th>State &amp; Local</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget constraints</td>
<td>30%</td>
<td>35%</td>
<td>26%</td>
</tr>
<tr>
<td>Competing priorities, other initiatives</td>
<td>14%</td>
<td>14%</td>
<td>19%</td>
</tr>
<tr>
<td>Complexity of internal environment</td>
<td>18%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>Lack of top-level direction and leadership</td>
<td>8%</td>
<td>13%</td>
<td><strong>18%</strong></td>
</tr>
</tbody>
</table>

*State & Local Gov*  
*State*  
*Local*

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>State &amp; Local Gov</th>
<th>State</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget constraints</td>
<td><strong>50%</strong></td>
<td>25%</td>
<td></td>
</tr>
</tbody>
</table>
Sources of Security Threats

The general hacking community is the largest source of security threats at public sector organizations, followed closely by careless/untrained insiders.

- General hacking community: 56%
- Careless/untrained insiders: 52%
- Foreign governments: 47%
- Hacktivists: 40%
- Malicious insiders: 32%
- For-profit crime: 27%
- Industrial spies: 20%
- Terrorists: 19%

Note: Multiple responses allowed
Sources of Security Threats by Organization Type

- State and local governments are significantly more likely than other public sector groups to mark the threat of the general hacking community (the top source of threats overall).

- Federal civilian agency respondents are more likely to indicate the general hacking community and careless insiders as a threat compared to defense.

- Significantly more federal respondents than education organizations indicate foreign governments and terrorists as threats. Defense respondents are more likely to note foreign governments.

<table>
<thead>
<tr>
<th>Source</th>
<th>Federal</th>
<th>State &amp; Local</th>
<th>Education</th>
<th>Defense</th>
<th>Civilian</th>
</tr>
</thead>
<tbody>
<tr>
<td>General hacking community</td>
<td>56%</td>
<td>63%</td>
<td>49%</td>
<td>46%</td>
<td>63%</td>
</tr>
<tr>
<td>Careless/untrained insiders</td>
<td>52%</td>
<td>51%</td>
<td>53%</td>
<td>41%</td>
<td>58%</td>
</tr>
<tr>
<td>Foreign governments</td>
<td>59%</td>
<td>46%</td>
<td>25%</td>
<td>68%</td>
<td>53%</td>
</tr>
<tr>
<td>Terrorists</td>
<td>23%</td>
<td>18%</td>
<td>11%</td>
<td>25%</td>
<td>22%</td>
</tr>
</tbody>
</table>
Sources of Security Threats – Federal Trend

The top three sources of security threats have remained the same for the federal audience since 2014. There are significant increases from 2019 to 2021 for threats from foreign governments, the general hacking community, and hacktivists.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign governments</td>
<td>34%</td>
<td>38%</td>
<td>48%</td>
<td>48%</td>
<td>52%</td>
<td>48%</td>
<td>59%</td>
</tr>
<tr>
<td>General hacking community</td>
<td>47%</td>
<td>46%</td>
<td>46%</td>
<td>38%</td>
<td>48%</td>
<td>40%</td>
<td>56%</td>
</tr>
<tr>
<td>Careless/untrained insiders</td>
<td>42%</td>
<td>53%</td>
<td>48%</td>
<td>54%</td>
<td>56%</td>
<td>52%</td>
<td>52%</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>26%</td>
<td>30%</td>
<td>38%</td>
<td>34%</td>
<td>31%</td>
<td>26%</td>
<td>42%</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>17%</td>
<td>23%</td>
<td>22%</td>
<td>29%</td>
<td>36%</td>
<td>29%</td>
<td>30%</td>
</tr>
<tr>
<td>For-profit crime</td>
<td>11%</td>
<td>14%</td>
<td>18%</td>
<td>17%</td>
<td>15%</td>
<td>20%</td>
<td>27%</td>
</tr>
<tr>
<td>Terrorists</td>
<td>21%</td>
<td>18%</td>
<td>24%</td>
<td>20%</td>
<td>25%</td>
<td>22%</td>
<td>23%</td>
</tr>
<tr>
<td>Industrial spies</td>
<td>6%</td>
<td>10%</td>
<td>16%</td>
<td>12%</td>
<td>19%</td>
<td>16%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Note: Multiple responses allowed

© 2021 Market Connections, Inc. © 2021 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED
Sources of Security Threats – State/Local + Education

The top three sources of security threats have remained the same for the SLED audience since 2019.

<table>
<thead>
<tr>
<th></th>
<th>State/Local 2019</th>
<th>State/Local 2021</th>
<th>Education 2019</th>
<th>Education 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>General hacking community</td>
<td>40%</td>
<td>63%</td>
<td>40%</td>
<td>49%</td>
</tr>
<tr>
<td>Careless/untrained insiders</td>
<td>52%</td>
<td>51%</td>
<td>52%</td>
<td>53%</td>
</tr>
<tr>
<td>Foreign governments</td>
<td>48%</td>
<td>46%</td>
<td>48%</td>
<td>25%</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>26%</td>
<td>43%</td>
<td>26%</td>
<td>32%</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>29%</td>
<td>36%</td>
<td>29%</td>
<td>33%</td>
</tr>
<tr>
<td>For-profit crime</td>
<td>20%</td>
<td>29%</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Industrial spies</td>
<td>16%</td>
<td>21%</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Terrorists</td>
<td>22%</td>
<td>18%</td>
<td>22%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Note: Multiple responses allowed

What are the greatest sources of IT security threats to your organization? (select all that apply)

© 2021 Market Connections, Inc. © 2021 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED
Impediments to Detection/Remediation of Security Issues

The top impediments to detection/remediation are insufficient training of IT staff and shortage of funding and resources. Lack of visibility into network traffic/logs or lack of central reporting and remediation are less of an issue.

Note: Multiple responses allowed

Which of the following are the greatest impediments to detection and remediation of security issues at your organization?
Concern About IT Security Threats Since 2020

Increasing concerns about foreign governments and the general hacking community are the largest sources of security threats at public sector organizations.

Compared to 2020, has your level of concern changed regarding the following sources of IT security threats?

- Decreased
- Remained the same
- Increased

- Foreign governments: 14% Decreased, 29% Remained the same, 56% Increased
- General hacking community: 4% Decreased, 44% Remained the same, 51% Increased
- For-profit crime: 13% Decreased, 43% Remained the same, 45% Increased
- Hacktivists: 9% Decreased, 49% Remained the same, 42% Increased
- Careless/untrained insiders: 20% Decreased, 39% Remained the same, 41% Increased
- Industrial spies: 13% Decreased, 53% Remained the same, 34% Increased
- Malicious insiders: 15% Decreased, 57% Remained the same, 28% Increased
- Terrorists: 16% Decreased, 56% Remained the same, 27% Increased
Concern About Security Breaches Since 2020

Increasing concerns about security breaches with ransomware, malware, and phishing top the list for public sector organizations.

- Ransomware: 10% decreased, 24% remained the same, 66% increased
- Malware: 6% decreased, 30% remained the same, 65% increased
- Phishing: 11% decreased, 27% remained the same, 63% increased
- Human error: 10% decreased, 41% remained the same, 49% increased
- User permission/credential abuse: 14% decreased, 51% remained the same, 35% increased
- SQL injection: 14% decreased, 55% remained the same, 31% increased
- Denial of service: 15% decreased, 55% remained the same, 29% increased
- Theft of equipment: 23% decreased, 51% remained the same, 26% increased

Note: Multiple responses allowed

Compared to 2020, has your level of concern changed regarding the following types of security breaches in 2021?

- Phishing: Federal 6%, State & Local 20%, Education 10%
- Denial of Service: Federal 12%, State & Local 22%, Education 15%
- Theft of equipment: Federal 25%, State & Local 24%, Education 15%

= statistically significant difference
Security Incidents and Events Since 2020

Approximately 6 out of 10 reported that time to detection and time to resolution has largely remained the same or worsened in 2021.
Overall Security Posture Since 2020

More than half of public sector organizations rate their security posture for fully remote and hybrid employees as improved.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Significantly/somewhat worse</th>
<th>About the same</th>
<th>Significantly/somewhat improved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully remote employees</td>
<td>19%</td>
<td>24%</td>
<td>57%</td>
</tr>
<tr>
<td>Hybrid employees</td>
<td>21%</td>
<td>29%</td>
<td>50%</td>
</tr>
<tr>
<td>Onsite employees</td>
<td>15%</td>
<td>37%</td>
<td>48%</td>
</tr>
<tr>
<td>[EDUCATION ONLY] Students</td>
<td>15%</td>
<td>46%</td>
<td>39%</td>
</tr>
<tr>
<td>[S&amp;L AND FEDERAL] Citizens served</td>
<td>18%</td>
<td>46%</td>
<td>36%</td>
</tr>
<tr>
<td>Vendors, contractors</td>
<td>20%</td>
<td>45%</td>
<td>35%</td>
</tr>
</tbody>
</table>

Compared to 2020, how would you rate your organization’s overall security posture regarding the following stakeholders?

© 2021 Market Connections, Inc. © 2021 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED
Importance of IT Solutions – Top 10 (Slide 1 of 3)

When rating the importance of IT security products, solutions, and services in mitigating risk to the organization, network security software rates highest. Of note, all protocols garnered high importance ratings of 50% and up.

<table>
<thead>
<tr>
<th>Product</th>
<th>Very/somewhat important</th>
<th>Neither important nor not important</th>
<th>Not at all/not very important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security software</td>
<td>77%</td>
<td>17%</td>
<td>6%</td>
</tr>
<tr>
<td>Policy and compliance</td>
<td>76%</td>
<td>19%</td>
<td>6%</td>
</tr>
<tr>
<td>VPN</td>
<td>76%</td>
<td>20%</td>
<td>5%</td>
</tr>
<tr>
<td>Firewall/UTM</td>
<td>76%</td>
<td>19%</td>
<td>5%</td>
</tr>
<tr>
<td>Access and information protection</td>
<td>76%</td>
<td>19%</td>
<td>6%</td>
</tr>
<tr>
<td>Authentication</td>
<td>75%</td>
<td>18%</td>
<td>8%</td>
</tr>
<tr>
<td>Privileged access</td>
<td>75%</td>
<td>17%</td>
<td>8%</td>
</tr>
<tr>
<td>Endpoint security software</td>
<td>74%</td>
<td>21%</td>
<td>6%</td>
</tr>
<tr>
<td>Server security</td>
<td>73%</td>
<td>20%</td>
<td>7%</td>
</tr>
<tr>
<td>IT education and training</td>
<td>73%</td>
<td>22%</td>
<td>6%</td>
</tr>
</tbody>
</table>

A greater proportion of federal respondents note 19 of the 30 solutions on the survey as important relative to state and local or education respondents.
Importance of IT Solutions (Slide 2 of 3)

When rating the importance of IT security products, solutions, and services, the following 10 protocols were rated in the middle of the IT protocols list.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Not at all/not very important</th>
<th>Neither important nor not important</th>
<th>Very/somewhat important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration services</td>
<td>8%</td>
<td>19%</td>
<td>73%</td>
</tr>
<tr>
<td>Antimalware</td>
<td>7%</td>
<td>21%</td>
<td>72%</td>
</tr>
<tr>
<td>Support security services</td>
<td>6%</td>
<td>23%</td>
<td>71%</td>
</tr>
<tr>
<td>Security device systems management</td>
<td>4%</td>
<td>25%</td>
<td>71%</td>
</tr>
<tr>
<td>Software vulnerability assessment</td>
<td>6%</td>
<td>23%</td>
<td>71%</td>
</tr>
<tr>
<td>Security suites</td>
<td>8%</td>
<td>22%</td>
<td>71%</td>
</tr>
<tr>
<td>Data loss prevention hardware</td>
<td>8%</td>
<td>22%</td>
<td>71%</td>
</tr>
<tr>
<td>Provisioning</td>
<td>8%</td>
<td>24%</td>
<td>70%</td>
</tr>
<tr>
<td>Device vulnerability assessment</td>
<td>8%</td>
<td>23%</td>
<td>70%</td>
</tr>
<tr>
<td>Forensics and incident investigation</td>
<td>9%</td>
<td>23%</td>
<td>69%</td>
</tr>
</tbody>
</table>
Importance of IT Solutions (Slide 3 of 3)

Rating at the bottom of the list of IT protocols is web content inspection software and consulting services.

- Data loss prevention software: 8% Not at all/not very important, 23% Neither important nor not important, 69% Very/somewhat important
- Single sign-on: 7% Not at all/not very important, 25% Neither important nor not important, 68% Very/somewhat important
- Managed security services: 8% Not at all/not very important, 25% Neither important nor not important, 67% Very/somewhat important
- Security information and event management: 6% Not at all/not very important, 27% Neither important nor not important, 67% Very/somewhat important
- Proactive endpoint risk management: 11% Not at all/not very important, 22% Neither important nor not important, 67% Very/somewhat important
- Hardware content management: 7% Not at all/not very important, 26% Neither important nor not important, 67% Very/somewhat important
- Messaging security software: 10% Not at all/not very important, 26% Neither important nor not important, 64% Very/somewhat important
- IDP/IPS: 6% Not at all/not very important, 31% Neither important nor not important, 64% Very/somewhat important
- Web content inspection software: 11% Not at all/not very important, 29% Neither important nor not important, 60% Very/somewhat important
- Consulting services: 10% Not at all/not very important, 34% Neither important nor not important, 56% Very/somewhat important

How important are the following IT security products, solutions, and services in mitigating risk at your organization?
Investment Priorities: IT Security

Investment priorities for IT security all rate as high priority for public sector organizations, with close to 70% of respondents placing intrusion detection/prevention and access management as their highest priority.

<table>
<thead>
<tr>
<th>Area</th>
<th>Low priority (1+2)</th>
<th>Neutral (3)</th>
<th>High priority (4+5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion detection and prevention</td>
<td>8%</td>
<td>24%</td>
<td>68%</td>
</tr>
<tr>
<td>Access management</td>
<td>7%</td>
<td>26%</td>
<td>67%</td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>8%</td>
<td>27%</td>
<td>65%</td>
</tr>
<tr>
<td>Security event and incident management</td>
<td>8%</td>
<td>27%</td>
<td>65%</td>
</tr>
<tr>
<td>Improve compliance</td>
<td>8%</td>
<td>27%</td>
<td>65%</td>
</tr>
<tr>
<td>Education and training</td>
<td>9%</td>
<td>28%</td>
<td>63%</td>
</tr>
<tr>
<td>Implementing a zero-trust framework</td>
<td>10%</td>
<td>30%</td>
<td>61%</td>
</tr>
</tbody>
</table>

What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?
Investment Priorities: Infrastructure

For infrastructure investment, public service organizations place remote access capabilities and collaboration tools as highest priority. All infrastructure investment options hold high priority in general.
Investment Priorities: IT Modernization

Like other investment priorities, IT modernization categories rate as high priority. Replacing legacy applications and migrating systems to the cloud hold highest importance.

- **Replace legacy applications**: 9% Low priority, 31% Neutral, 60% High priority
- **Migrate systems to the cloud**: 9% Low priority, 31% Neutral, 60% High priority
- **Virtualize and consolidate datacenter**: 15% Low priority, 27% Neutral, 59% High priority
- **Utilize digital services**: 11% Low priority, 31% Neutral, 59% High priority
Investment Priorities: Customer Experience + Digital Transformation

For customer experience investment, IT services management leads. And for digital transformation, implementing stakeholder platforms or portals also rate with priority among public sector organizations.
White House Cyber Security Executive Order Familiarity

Most public sector organizations are familiar with the Cyber Security Executive Order. This familiarity is across federal, state and local, and education organizations.
## Executive Order’s Impact on Improving Cybersecurity

The objectives of the Cyber Security Executive Order that are ranked as most impactful to improving organizations’ cybersecurity and network protection are improving investigative and remediation capabilities and improving barriers to sharing threat information between government and private sectors.

### Ranks of Objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>Average Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve investigative and remediation capabilities</td>
<td>15%</td>
<td>10%</td>
<td>20%</td>
<td>19%</td>
<td>12%</td>
<td>10%</td>
<td>14%</td>
<td>3.89</td>
</tr>
<tr>
<td>Improve barriers to sharing threat information between government and the private sector</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>23%</td>
<td>12%</td>
<td>3.91</td>
</tr>
<tr>
<td>Create a standard playbook for responding to cyber incidents</td>
<td>17%</td>
<td>13%</td>
<td>15%</td>
<td>14%</td>
<td>15%</td>
<td>10%</td>
<td>17%</td>
<td>3.95</td>
</tr>
<tr>
<td>Improve detection of cybersecurity incidents on networks</td>
<td>14%</td>
<td>10%</td>
<td>16%</td>
<td>19%</td>
<td>17%</td>
<td>8%</td>
<td>16%</td>
<td>4.01</td>
</tr>
<tr>
<td>Improve software supply chain security</td>
<td>14%</td>
<td>14%</td>
<td>15%</td>
<td>13%</td>
<td>16%</td>
<td>16%</td>
<td>13%</td>
<td>4.03</td>
</tr>
<tr>
<td>Establish a cybersecurity safety review board</td>
<td>15%</td>
<td>13%</td>
<td>15%</td>
<td>14%</td>
<td>15%</td>
<td>14%</td>
<td>15%</td>
<td>4.04</td>
</tr>
<tr>
<td>Modernize and implement stronger cybersecurity standards</td>
<td>12%</td>
<td>16%</td>
<td>12%</td>
<td>12%</td>
<td>16%</td>
<td>20%</td>
<td>13%</td>
<td>4.18</td>
</tr>
</tbody>
</table>

---

The White House’s Cyber Security Executive Order includes multiple objectives. Regardless of your familiarity with the Executive Order, please rank the perceived impact of each objective as it pertains to improving your organization’s cybersecurity and network protection. (Rank 1 as the most impactful, 2 is the second most impactful, and so forth.)

© 2021 Market Connections, Inc. © 2021 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED
SLED: Likelihood of Incorporating Federal Best Practices

Among state and local governments and education respondents, 86% are likely to refer to or incorporate best practices and activities based on the objectives of the Cyber Security Executive Order. Education organizations, particularly K-12 schools, are significantly more likely to incorporate best practices.

- Among state and local government respondents, 80% are very or somewhat likely to refer to or incorporate best practices, compared to 91% of education respondents.
- Among K-12 schools, 98% are very or somewhat likely to refer to or incorporate best practices, compared to 84% of higher education institutions.

How likely is your organization to refer to or incorporate cybersecurity best practices and activities put forth by the federal government, like those outlined in the Executive Order noted previously?
Using a Zero-Trust Approach to IT Security – Motivators

More than one-third have a formal strategy in place and are actively implementing the zero-trust approach. Education and defense respondents are more motivated by data protection, local governments by breach protection.

**KEY MOTIVATORS**

<table>
<thead>
<tr>
<th>Top 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach protection</td>
</tr>
<tr>
<td>Data protection</td>
</tr>
<tr>
<td>Reduction of endpoint &amp; IoT security threat</td>
</tr>
<tr>
<td>Compliance with the White House Cyber Security Executive Order</td>
</tr>
<tr>
<td>Reduce insider threats</td>
</tr>
<tr>
<td>Movement to a hybrid cloud environment</td>
</tr>
</tbody>
</table>

**Is your organization currently using or considering a zero-trust approach to IT security? IF YES What are the key motivators for your organization to implement or consider a zero-trust approach?**

- Federal
  - Breach protection: 71%
  - Data protection: 64%
- State & Local
  - Breach protection: 73%
  - Data protection: 64%
- Education
  - Breach protection: 67%
  - Data protection: 78%
- Defense
  - Breach protection: 70%
  - Data protection: 71%
- Civilian
  - Breach protection: 61%
  - Data protection: 57%
- State
  - Breach protection: 61%
  - Data protection: 61%
- Local
  - Breach protection: 82%
  - Data protection: 66%
Using a Zero-Trust Approach to IT Security – Deterrents

Nearly one-fifth are not actively using or considering a zero-trust approach. Key deterrents cited are lack of staff expertise, other IT initiatives taking priority, and no formal compliance mandates.

**KEY DETERENTS**

- Lack of IT/security staff expertise: 57%
- Other IT initiatives take priority: 55%
- No formal compliance mandates: 54%
- Lack of policies and processes: 42%
- Solutions are too costly: 38%
- Leadership/upper management doesn’t see the need: 30%
- Uncertainty over which zero-trust model to follow: 24%
The importance of implementing a zero-trust approach is high among all public sector organizations. Federal civilian respondents are more likely to think zero trust is important to adopt.
Overall, public sector organizations are familiar with the principle of least privilege, and the education sector is significantly more familiar.
Timeframe for Implementing PoLP

Nearly one third are actively implementing the principle of least privilege. Reducing the overall attack surface and stopping the spread of malware are the seen as the greatest benefits.

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We're already implementing it</td>
<td>29%</td>
</tr>
<tr>
<td>Within the next six months</td>
<td>25%</td>
</tr>
<tr>
<td>Within 7-12 months</td>
<td>16%</td>
</tr>
<tr>
<td>Not sure of timeframe but</td>
<td>26%</td>
</tr>
<tr>
<td>considering it</td>
<td></td>
</tr>
<tr>
<td>We're not considering it</td>
<td>3%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Benefits**

- Reduces of the overall cyberattack surface: 75%
- Stops the spread of Malware: 72%
- Reduces costs by saving time and money in managing users securely: 63%
- Helps demonstrate compliance with a full audit of privileged activities: 50%
- Improves end-user productivity: 40%

**Comparative Analysis**

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Federal</th>
<th>State &amp; Local</th>
<th>Education</th>
<th>State</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demonstrates compliance</td>
<td>55%</td>
<td>37%</td>
<td>51%</td>
<td>53%</td>
<td>27%</td>
</tr>
<tr>
<td>Stops Malware</td>
<td>69%</td>
<td>78%</td>
<td>73%</td>
<td>63%</td>
<td>88%</td>
</tr>
</tbody>
</table>

*Statistically significant difference*
Teleworking - Before COVID-19, Now, and in the Future

Before COVID-19, about half of employees worked remotely sometimes, with close to 20% often/always doing so. Currently, about two-thirds often/always work remotely, and is expected to stay at that level in the future.

<table>
<thead>
<tr>
<th>MEANS</th>
<th>Before COVID</th>
<th>Currently</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>3.12</td>
<td>4.73</td>
<td>4.58</td>
</tr>
<tr>
<td>Defense</td>
<td>2.79</td>
<td>4.39</td>
<td>4.29</td>
</tr>
<tr>
<td>Civilian</td>
<td>3.33</td>
<td>4.96</td>
<td>4.77</td>
</tr>
<tr>
<td>State &amp; Local</td>
<td>3.25</td>
<td>4.69</td>
<td>4.51</td>
</tr>
<tr>
<td>Education</td>
<td>3.45</td>
<td>4.83</td>
<td>4.62</td>
</tr>
<tr>
<td>TOTAL</td>
<td>3.23</td>
<td>4.74</td>
<td>4.57</td>
</tr>
</tbody>
</table>

Please indicate your organization's general level of employee teleworking/working remotely before the COVID-19 pandemic, currently, and how you envision teleworking in the future.
The main difficulty is in finding and hiring qualified IT employees and then retaining them.

FEDERAL CIVILIAN

We are very concerned about our cybersecurity.

K-12 EDUCATION

We are a small agency, so remote work was easier than expected.

FEDERAL CIVILIAN

The vast majority of our work is done on classified information systems. As much as we would like to embrace telework or remote operations, it is not physically possible.

DEFENSE / MILITARY

I think for an organization that has to balance the need to access data remotely due to Covid, plus balance against the need to access a physical office to access certain systems, and the demand from senior leadership to make these systems which should never be remote, remote... rough water are ahead.

FEDERAL CIVILIAN

Remote access is improving and will continue to be a priority.

DEFENSE / MILITARY

A security challenge will be putting trust in hardware that is procured from overseas. The US government’s push for the reshoring of electronics manufacture that began some years ago and has since gained momentum. If you and your customers are based in the United States, reshoring can help alleviate some of the supply chain unknowns. The looming question is how many supply chain unknowns will remain unknown?

DEFENSE / MILITARY

Manpower shortages.

HIGHER EDUCATION

Please feel free to share any other comments or concerns regarding your organization’s unique security challenges or success stories.
Key Takeaways

The top three sources of security threats remain the same as in previous years. The greatest increase in concern is from threats from foreign governments.

• Overall, the general hacking community is the largest source of security threat in the public sector. Careless or untrained insiders is still a top three source but has remained stable year over year. Foreign governments is also among the top three sources with more federal government respondents noting it.

• Federal government and SLED respondents’ indications of the general hacking community as a threat source has significantly increased.

• Concern about ransomware, malware and phishing has increased for most public sector respondents.
Key Takeaways

Most public sector respondents realize the importance of IT security solutions and prioritize their investments highly in the next 12 months.

- All IT security solutions received importance ratings of 50% and more. At the very top of the list is network security software. Policy and compliance, VPN, firewall/UTM, and access and information protection all tied for second most important.

- All investment priorities received high priority ratings for public sector organizations. For IT security, almost 70% of respondents placed intrusion detection and prevention and access management top of the list.

- For infrastructure investments, remote access capabilities and collaboration tools were rated as highest priority.

- IT modernization investment priority leans toward replacing legacy applications and migrating systems to the cloud.

- When it comes to customer experience, IT services management holds investment priority. And for digital transformation, implementing stakeholder platforms and portals is key.
Key Takeaways

Public sector organizations in all segments are aware of the White House Cyber Security Executive Order.

- Ninety percent of respondents are familiar with the White House Cyber Security Executive Order.

- The objectives of the Cyber Security Executive Order that are ranked as most impactful to improving organizations’ cybersecurity and network protection are improving investigative and remediation capabilities and improving barriers to sharing threat information between government and private sectors.

- Among SLED organizations, about 20% are very likely and 66% somewhat likely to adopt cybersecurity best practices and activities from the Cyber Security Executive Order. Education organizations are significantly more likely to implement.
Key Takeaways

The awareness and adoption of zero trust has increased since 2019.

A zero-trust approach is already formally in place or modeled for most organizations because of its key motivators and perceived importance.

• More than three-fourths of public sector organizations use a formal or informal zero-trust approach.

• Motivators for using zero trust include breach protection and data protection, while lack of IT/security staff expertise is the key deterrent.

• All types of public sector organizations give zero trust importance, with federal civilian respondents citing significantly higher importance to the approach.

• Public sector organizations are familiar with the principle of least privilege (PoLP), especially those in education.

• The timeframe of having PoLP in place is already implemented or within the next 12 months for 70% of respondents.
Key Takeaways

The COVID-19 pandemic drastically changed the work environment for many public sector employees. While some employees have returned to the physical office, respondents expect large numbers teleworking in the future.

• Before COVID-19, about half of employees worked remotely sometimes, with close to 20% often/always doing so.

• Currently, about two-thirds often/always work remotely, and is expected to stay at that level in the future.

• Current and future teleworking is significantly higher for federal civilian organizations.

• More than half of respondents rate their security posture for fully remote and hybrid employees as significantly or somewhat better.
Contact Information

Laurie Morrow, VP, Research Strategy, Market Connections, Inc.
LaurieM@marketconnectionsinc.com
571-257-3845

Lisa M. Sherwin Wulf, Vice President of Americas Marketing, SolarWinds
Lisa.SherwinWulf@solarwinds.com
703-386-2628

Jessica Primanzon, Director of Marketing, SolarWinds
jessica.primanzon@solarwinds.com
301-672-5351

[www.solarwinds.com/government](http://www.solarwinds.com/government)
LinkedIn: SolarWinds Government