# Security challenges for state and local government IT departments

**Increasing security risks in state and local government IT threaten the functioning of government services and the digital safety of constituents and employees.**

## Security vulnerabilities in public-sector IT

**92%** of government respondents in a recent survey will use sensitive data in an advanced technology over the coming year.

**96%** are aware of vulnerabilities in their cybersecurity.[1]

**#3** top target of data breaches in 2017: public-sector organizations.[2]

## Risks of shadow IT in the cloud

**928** is the average number of unsanctioned cloud apps in state governments.

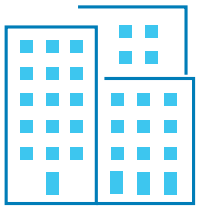
**25%** of the data in these apps is shared internally or externally.

Organizations experience an average of **14.8** insider threat incidents each month.[3]

## Shortage of security professionals

**350,000** cybersecurity positions went unfilled in the U.S. during 2017.

By 2019, the global workforce shortage in cybersecurity professionals is predicted to be as much as **2 million.**[4]



## Cyberespionage in the public sector

**64%** of the incidents of data breaches and ransomware in state and local government have espionage as their main motive.[6]

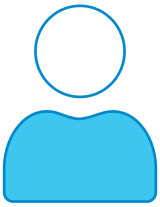
**21,000** security incidents were reported among 92 public-sector organizations.

**230** incidents resulted in a confirmed data breach.

**41%** of the stolen data was personal.

**90%** or more of the actors were connected to foreign governments.

**60%** of the data breaches took years to discover.



## Keeping security top of mind

**5 million** people work for state governments.

**14 million** people work for local governments.

**95%** of cybersecurity attacks are exacerbated by human error or by a lack of security awareness among employees.[5]

## Escalating ransomware threats

**#1 target** of ransomware in 2017: government organizations.[7]

In 2017, ransomware became the **5th-most** common type of malware (it ranked 22nd in 2014).

**8 years** of digital evidence was lost by a police department in Texas that refused to pay a ransom.[8]

[1] https://betanews.com/2017/04/27/us-government-data-breach/
[2] Verizon, "2017 Data Breach Investigations Report," 10th edition, April 2017.
[3] McAfee, "Cloud Adoption & Risk Report 2019," https://www.skyhighnetworks.com/cloud-report/
[4] www.herjavecgroup.com/wp-content/uploads/2017/06/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf
[5] www.govtech.com/security/Can-Security-Awareness-Training-Change-Behavior-and-Reduce-Risk.html
[6] Verizon, 2017 Data Breach Investigations Report.
[7] Ibid.
[8] https://nakedsecurity.sophos.com/2017/02/01/eight-years-worth-of-police-evidence-wiped-out-in-ransomware-attack/
[9] Ponemon Institute, "The Economic Risk of Confidential Data on Mobile Devices in the Workplace," February 2016.

Learn more about Dell EMC SLG resources and solutions
Contact a Dell EMC government expert at 1 (866) 438-3622
Connect with @DellEMCSLG

DELL EMC | intel