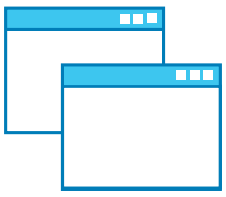
State and local governments chart their path toward improved digital security

State and local governments are under attack from cyberespionage and malware, and they are exposed to a broad variety of security risks. Are your approaches to IT security making your government organization more vulnerable? If so, strong best practices and successful government security initiatives in progress highlight a path forward.

New approaches are needed to make government IT less vulnerable

In managing digital security, many IT leaders in state and local government rely on counterproductive tactics or don't implement measures that could strengthen their security, such as:



Prioritizing preventive tools that cannot protect data once a digital intruder has entered systems

Relying too much on one-time audits and annual risk management reviews, giving criminals far too much time to prepare and execute attacks

Using compliance as a security benchmark, which results in what is considered the lowest level of risk management and compliance maturity

Failing to take advantage of existing controls and easily available tools, such as encryption for data at rest, multi-factor authentication, routine patches, automated threat analysis or user education

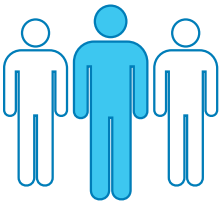
Transforming digital security in the public sector

Some governments are already transforming their cybersecurity management by taking the following actions:

Create resilient security from the ground up with data protection on all servers, storage and client devices. User access and identity management rely on encryption and stringent controls. A process is in place to recover data after a breach.

Implement transparent, adaptable security measures that enable security managers to assess the threat landscape, identify vulnerabilities, and create needed programs and controls. IT can create a specifically designed security operations center and use automation and analytics to accelerate responses and deflect threats.

Practice unified risk management to identify and prioritize risk in context, synchronize security practices across the organization, and increase their control in security and compliance management.



Enroll the expertise of trusted security experts who can extend your team in an advisory role and provide timely intelligence regarding the potential threats that your organization faces.

7 best practices for cybersecurity in state and local government

We have identified several effective tactics that can help improve digital security in the public sector:

1. **Heed the basics**
   Keep policies, procedures and documentation current and align your security program with them.

2. **Perform a thorough risk assessment**
   Identify your most sensitive data, review its protection and compare your security practices to organizational policies and industry best practices.

3. **Implement continuous risk assessment**
   Conduct a weekly risk-management review for critical services and run what-if scenarios to test cybersecurity and incident-response plans.

4. **Centralize governance**
   When state and local IT teams adopt systems that range across jurisdictions, centralized cybersecurity governance can ensure full, accurate risk assessment and consistent security controls.

5. **Build a culture of security awareness**
   Executives, senior staff and all other system users need to receive security awareness training and understand how they can help mitigate risk.

6. **Establish metrics and scoring dashboards**
   Identify goals and indicators for measuring improvement in your security management. Run penetration and other tests to verify that your measures are working, and track progress over time.

7. **Choose experienced, stable vendors**
   If you choose cybersecurity solutions, give priority to the providers that can offer deep experience in public-sector technology and security, that share a long-term technology roadmap, and that are most likely to be viable years from now.

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