4 Security Considerations for Better Organizational Resiliency

The recent global pandemic taught us that anything can happen. Yet whatever the event—from weather emergencies to natural disasters and local governments must continue to serve their communities and provide essential services. Technology teams inside government agencies are gathering and analyzing data to help them stay agile and deliver the right response to any situation. Yet the more data-driven they become, the more enticing they are for cyberattackers.

4 security initiatives that build organizational resilience

1. Adopt a Zero Trust architecture (ZTA)
   - ZTA helps you better secure data and supports greater productivity, organizational agility, and improved user experiences.
   - Why it’s important: With the growth of remote and hybrid work, security methods based on the network perimeter are no longer effective.

   **AT LEAST 113** state and local governments in the U.S. were affected by ransomware in 2021.
   **$665,000 TO $40.53 MILLION** is the total cost to government agencies from recovering data lost or stolen by ransomware.
   **22 DAYS** is the average length of disruption after ransomware attacks on businesses and organizations.

2. Modernize applications
   - Modern apps provide the ability to offer new features and functionality to citizens and workers while mitigating cyber risks.
   - Why it’s important: The security threats that exist today didn’t exist when legacy applications were designed, so many are vulnerable to techniques and exploits that attackers can use to breach government systems.

   **2 OF THE TOP 3** cybersecurity challenges are related to how government agencies manage access to applications.

3. Expand the use of identity and access management (IAM)
   - IAM helps IT teams spend less effort, time and money on manually managing network access while reducing the risk of internal and external data breaches.
   - Why it’s important: Traditional methods based on different sign-ons for every app or system create management headaches and security risks.

   **48.4%** say they use separate solutions for issues such as endpoint security, network security, and application security.

4. Migrate to one or more clouds
   - Using the cloud—or multiple clouds—provides improved security, better failover options, and enhanced disaster recovery.
   - Why it’s important: If all of your apps and data are located in a single, on-premises data center (or even a single cloud environment), your agency is vulnerable in the case of failure or another kind of disastrous event.

   **LEARN MORE**

VMware solutions help you protect citizen data and grow resiliency

VMware is a trusted partner for state and local government agencies. No matter where you are in your security journey, VMware can help you determine where you are now, where you want to be, and how to get there.

Our security solutions can help you improve your security posture from endpoint to app to cloud to network.

Find out why state and local governments are securing their environments with VMware.

---