GOVERNMENT SOLUTIONS

Keeping governments secure from the inside out

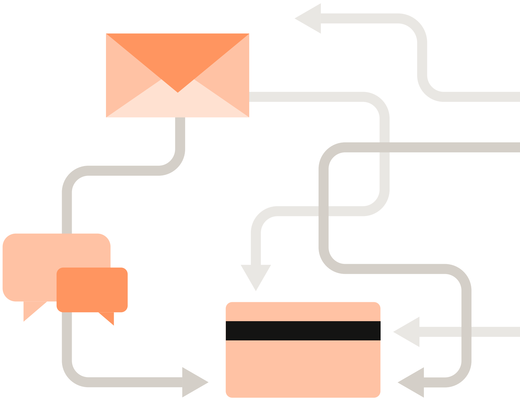
Governments must be critical of their third-party vendor relationships when it comes to safeguarding critical data and networks, but it's equally important to keep their own infrastructure secure.

Visible lines of defense

Without a full picture of their own risk surface, governments could be severely disadvantaged in the event of a data breach. This lack of insight makes them more susceptible to cyberattacks such as ransomware.

41% of American city governments do not have information security programs strong enough to protect their data assets.

Organizations with a RiskRecon by Mastercard cybersecurity risk rating of a **D or F** are **40 times more likely to experience a ransomware attack.**



A healthy balance

The overall cybersecurity risk rating and cyber hygiene of governments improve when they are properly aligned with international cybersecurity standards, including cryptographic controls and dimension frameworks, according to RiskRecon and Oxford University research.

Safeguarding critical infrastructure

RiskRecon enables governments to navigate complex and evolving cybersecurity safeguards by helping them preemptively identify, prioritize and reduce risk within their own organizations and amongst their third-party relationships.

In 2022, this approach helped RiskRecon customers, including many government organizations, flag

144 million vulnerabilities

To learn more, visit riskrecon.com