CASE STUDY

www.the-atlas.com

IT Department establishes centralized cybersecurity roadmap by leveraging CIS18 framework

CHALLENGE

Crafting a uniform approach to cybersecurity strategy in county government is particularly challenging given the wide breadth and depth of requirements across a range of security domains; data privacy, availability of critical resources and systems, mandates for special protection of officially designed critical infrastructure, and even variances in acceptable risk tolerance levels by agency, to name a few.

Over time, the variance in needs in Contra Costa County resulted in a decentralized approach to cybersecurity across the county's 28 agencies. This dynamic is common in many County governments and fosters an environment with an inconsistent implementation of controls and a lack of standardization in securing systems and data. Lacking a way to collaborate and communicate effectively towards a common set of priorities, agencies approach their cyber challenges in silos, increasing overall costs, and potentially, risk.

AT A GLANCE

Contra Costa County has 28 government agencies, each with different cyber needs. This left their approach to cybersecurity decentralized. After completing a CIS18 framework analysis, the county set a clear, long-term strategy designed to develop cyber resilience.

SOLUTION

To address this, Contra Costa County utilized the professional services of a trusted industry partner, AT&T Cybersecurity, to provide an objective assessment of the cybersecurity program against the CIS18 controls framework.

The Contra Costa County security team approached the challenge with a novel strategy in mind: leading by example in the central information technology office. Rather than attempting to dictate to their semi-autonomous agencies by policy, they set out to showcase success defined as reduced risk and improved capability maturity in the smaller central environment. Their proactive security and best practices then developed a standardized approach to cybersecurity for all agencies to adopt willingly and enthusiastically. This also served to build consulting, assessment, and control capabilities of the newly developed security team, and the partner service providers that they work with. This collective force could then serve to guide others within the organization in their own unique challenges.

Beginning with the establishment of a baseline of controls using the Center for Internet Security (CIS) Critical Security Controls, the County security team was able to identify the greatest areas of risk in their environment, shore up gaps and weaknesses in their program, and set a long-term strategy that had the greatest return on investment for the citizens of Contra Costa County.

This solution has served to help provide direction and alignment of resources around a standardized and understandable "security baseline" for the organization, and ensure the collective team is moving jointly in a shared direction

CASE STUDY

www.the-atlas.com

IT Department establishes centralized cybersecurity roadmap by leveraging CIS18 framework

OUTCOMES

Outcome 1

Long-term strategic cybersecurity roadmap and plan developed after risk assessment

Outcome 2

Efficient budgeting and resourcing for the county through a centralized strategy

Outcome 3

Improved collaboration and alignment of initiatives across IT, cyber, and business thanks to baseline controls outlined by the Center for Internet Security (CIS)

LESSONS LEARNED

Lesson 1

Security risk management does not have to be complex.

Lesson 2

A team approach within government as well as public private coordination is necessary to achieve success.

Lesson 3

Bringing in an external partner with lots of private sector experience managing cyber risks to do an objective audit can help a country modernize more quickly.

Lesson 4

Federal funding, ARPA and IIJA included, can be used for projects, including this one, that build resilient cybersecurity infrastructure.

CHAMPION

Assistant CIO and CISO

FINANCING

General Fund but counties and cities can use new IIJA Funding for this work!

LEARN MORE

AT&T Cybersecurity

CIS18 Security Best Practices

AT&T

THE ATLAS