SecureWorks

STATE GOVERNMENT REVISES OUTDATED POLICIES IN ACCORDANCE WITH NIST STANDARDS

Existing policies aligned to ISO/IEC 27002 standards were up to five years old. With an increasingly challenging threat landscape, the state government knew it had to update security policies to protect its people and public services.

Industry: Government | **Country:** United States | **Employees**: 50,000+

BUSINESS NEED

With aging security policies—many orphaned—a state's umbrella IT agency wanted to strengthen cyber safeguards with policies updated to NIST federal government standards.

SOLUTION

The IT agency developed and deployed 23 new policies—with specific owners—to cut vulnerabilities to state operations, all with help from SecureWorks Security and Risk Consulting.

BENEFITS

- Strengthened overall security posture, reducing disruption risks
- Increased visibility into security policies and governance
- Boosted organizational security awareness and accountability
- Updated policies to address new technologies and threats
- Raised overall maturity of state's cybersecurity program

PRODUCTS | Security and Risk Consulting

SECURITY AND RISK CONSULTING

With tens of thousands of civil service employees across its nearly 200 agencies, the government of this large U.S. state could qualify as a Fortune 500 company. Like all large organizations, governments rely on information technology to efficiently and effectively serve the needs of the state's millions of citizens. However, given their high profile, wide range and volume of data, all governments are a hot, and sometimes easy, target for threat actors intent on cybercrime and hacktivism.

Data breaches or intrusions into any state government agency network can compromise PII, PHI, data and physical safety of their citizens, and disrupt the delivery of critical public services. In one recent incident, the state was hit with a denial-of-service attack and this incident impacted the operations of several state agencies, limiting their ability to deliver services.

Many governments have embraced the adoption of transformative technologies such as cloud, social media and mobile platforms. While these technologies allow governments to connect with and provide higher levels of transparency and service to their citizens, they can increase cyber risks, such as ransomware attacks.

SECURITY PRACTICES ACROSS AGENCIES NEED MORE CONSISTENCY

As security continues to be ever more of a focus – moving from being a technology to a business imperative, the underlying concern around finding the right people is set to become even more urgent. For the past four years, information security topped the list of skills shortages in the IT industry. Organizations need experienced security experts who can perform functions that cannot be automated, such as a strong understanding of security processes and methodology.

With an expertise shortage in InfoSec, the team from the state's umbrella IT agency has to cover a wide range of responsibility with a limited amount of time and staff. Some of their responsibilities include developing the state's IT strategy, technology roadmaps and best practices for disaster recovery and business continuity. Among those and many other responsibilities are security policies, governance and accountability.

Although the state's existing policies were written to ISO/IEC 27002 information security standards, they were not current. Some were over five years old and most lacked owners responsible for enforcement, governance and current content. Inconsistencies in graphic design, voice and tone were not user-friendly and made the policies seem as if they came from different sources. As a result, security practices were unevenly applied across the various state agencies and their disparate technology platforms.

SECURITY POLICY NEEDED UPDATING

With its own resources of staff so limited, the IT agency knew it did not have the time to undertake the end-to-end review and gap analysis of its security policies that were required. At the same time, it wanted to revise and reissue all its policies in compliance with the security controls spelled out in Special Publication 800-53, Revision 4, of the National Institute of Standards and Technology (NIST).

NIST standards were established to assist U.S. federal agencies in implementing the Federal Information Security Management Act of 2002. While ISO/IEC 27002 standards are more oriented to audit compliance with security practices, the NIST 800-53 standards more clearly define applications of security technologies and baselines for IT operations and governance.

The agency turned to the private sector for help in conducting the activities needed to publish a completely updated information security manual. After issuing an RFP and carefully evaluating respondents, the state chose SecureWorks for its Security and Risk Consulting (SRC) services.

CHOOSING SECUREWORKS FOR EXPERTISE AND EXPERIENCE

Deciding factors were the expertise and experience of SecureWorks in helping large organizations, especially governments and their agencies, identify security gaps and remedy them with industry-leading best practices. In addition, the agency valued how SecureWorks can also address business processes, regulatory needs, governance practices and appropriate strategies for risk management.

During the six-month engagement, the SecureWorks SRC team followed a proven delivery methodology called FACTS – Flexible, Align, Communicate, Transfer and Support. This aligns with two globally recognized project management standards: PRINCE2 (Projects IN Controlled Environments) and the Project Management Body of Knowledge (PMBOK® Guide) of the Project Management Institute (PMI).

The methodology ensures timely execution of activities to meet scheduled milestones. It also facilitates setting and meeting expectations, aided by frequent communications. The SecureWorks team included a full-time project manager, plus two experienced security analysts and a senior security advisor.

PROVEN, PHASED APPROACH OVER SIX MONTHS

The first phase involved interviews with key stakeholders as well as a thorough review and gap analysis of the existing ISO/IEC 27002-based policies. A target architecture and template for the new manual was established. This provided a document version history, a consistent graphic design, periodic reviews and policy ownership.

Next, the work of migrating existing policies from their ISO/IEC 27002 framework to NIST 800-53 began. The first 18 policies were:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Service Acquisition
- System and Communications Protection
- System and Information Integrity
- Privacy

Another five policies were added later. Additionally, the SRC team conducted a "cross-walk" exercise with all stakeholders. This mapped the old policies against the new. In effect, it provided the group with both a valuable project checkpoint as well as initial training in the new security manual's contents.

Going beyond the scope of work, SecureWorks also provided the agency with guidance on security requirements for international travel, cloud and mobile computing. This additional counsel underscored the consultant role SecureWorks brings to all its client engagements.

SECURITY STRENGTHENED, RISK REDUCED

As of the writing of this case study, the new security policy manual and its policies have been fully updated to NIST 800-53 standards, policy owners identified and governance established. The manual has been published and communicated to all those responsible for IT in the state's many agencies. This has given security policies much-needed visibility and raised organization awareness of their importance. The new policies also better addressed new technologies and threats.

Most importantly, the new policies have helped the state to strengthen its overall security posture, while reducing the risks of disruptions due to security breaches. The successful completion of this project has also raised the overall security of the state's cybersecurity program, providing greater peace of mind for those responsible for IT and risk management.

INCREASING SECURITY MATURITY EVEN FURTHER

In an effort to take the maturity of its security program to an even higher level, the state has chosen SecureWorks to help augment their security program with a Security Residency and Managed Security Services.

This program, with both strategic and tactical elements, can help the agency identify and address emerging security needs in what is, effectively, an ongoing conversation between its staff and SecureWorks. As the latter actively monitors the state's cybersecurity model, unknown vulnerabilities can be discovered and addressed before threat actors can take advantage of them. With this approach, the state will become much more proactive in executing its cyber safeguards.