FORTRA™

CASE STUDY (TRIPWIRE)

State of Iowa

Stronger Security Fortra's Tripwire IP360 and the Critical Security Controls

With today's growing and ever-changing threat landscape, the need for a strong cybersecurity initiative is apparent now more than ever. According to the 2014 US State of Cybercrime Survey conducted by PwC, "most organizations' cybersecurity programs do not rival the persistence, tactical skills and technological prowess of today's cyber adversaries." But how can they? With so many standards, rules, regulations and policies to implement and follow, it's hard to know where to start.

Jeff Franklin, the State of Iowa's Chief Information Security Officer, had that very same problem. At the time of his hire in 2009, Iowa was primarily focusing its security approach on the ISO 27000 series, a popular risk assessment framework for many state governments. While ISO 27000 provided a good measure of security, it lacked a critical operational aspect that was needed for the State of Iowa's complex environment. The state needed a more technical, systematic and reliable way to identify its vulnerabilities and real risks to determine their overall risk status. Something new needed to be implemented.

It was decided that an operational approach to security was in order. In partnership with the Iowa Homeland Security and Emergency Management, Iowa adopted the "Top 20" Critical Security Controls (CSC) from the Council on CyberSecurity as the state's risk management framework. An assessment of the CSC, a risk assessment framework that could identify and address the security gaps that remained after performing threat management and vulnerability scanning, showed that the standards could grow with the state.

This framework would help the state improve security now and over the long term. The Information Security Office needed to make some immediate security improvements—some quick wins to show improvement. Previous state risk audits indicated that vulnerability management (VM), Control 4 of the CSC, would provide the biggest cybersecurity gains for the investment. Based on this information, the state leveraged funds from a Department of Homeland Security (DHS) grant to launch a pilot project around VM.

AT-A-GLANCE

Organization State of Iowa

Industry Government

SOLUTION

Fortra's Tripwire® IP360™

BENEFITS

- Vulnerability risk scores reduced by over 50% across most state agencies
- VM solution Tripwire® IP360™ deployed to over 100 government entities
- Project VM coverage slated to more than double in size—from 20,000 to 40,000 IP addresses
- State-wide visibility to all software and hardware gained through inventory capability, meeting Controls 1 and 2 of the CSC
- Common risk scoring and metrics among state entities instituted, providing understanding of the state's security risk posture

Adopting the CSC— a More Operational Security Framework

The state selected the CSC as its framework because it provides a prioritized list of 20 controls that if implemented, greatly improve an organization's risk posture against today's real-world threats. The controls also provide a highly operational approach compared to other risk management frameworks by not only describing security best practices but also providing the means to verify that these practices are in place.

five, it should be Control 4, vulnerability management. He bases this belief on the state's experience implementing their VM pilot project using Tripwire® IP360™, but also because a byproduct of implementing VM is meeting Controls 1 and 2—creating an inventory of authorized and unauthorized devices and software.

A VM Pilot Project that Quickly Proves Its Value

In 2011, the State of Iowa began the process of implementing their selected vulnerability management solution. Funding from a Department of Homeland Security (DHS) grant and managed through Iowa's Homeland Security and Emergency Management Division was critical for the project's success. This funding enabled the state to implement a VM project, which the Office of Information Security had determined could make the biggest impact on state cybersecurity risk. Vulnerability management identifies system weaknesses (such as out-of-date security patches or non-standard configurations) that allow attackers to infiltrate systems. Many security professionals consider controls like VM simply good housekeeping, because they take care of the biggest security problems first.

> *"Iowa and other states have changed from security offices that were policy-based to operational. That's because as the climate has changed and cyber attacks are becoming more sophisticated and frequent, that doesn't suffice anymore. You have to have continuous testing and measurable results. That operational piece has to be there. The CSC provides that operational aspect to our risk assessment. That's why we introduced the CSC."*
> —**Jeff Franklin**, CISO, State of Iowa

Preventing the Majority of Incidents with Controls 1–5

While the state does parts of each of the CSC—for example, pen testing and security awareness training—its main focus is the top five controls. By focusing on the first five, Franklin notes, you can address a majority of potential incidents.

The first five controls are:

Control 1: Inventory of Authorized and Unauthorized Devices

Control 2: Inventory of Authorized and Unauthorized Software

Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Control 4: Continuous Vulnerability Assessment and Remediation

Control 5: Malware Defenses

According to Franklin, "The first five controls directly protect the organization and can make a difference in preventing a real breach, compared to implementing some of the other controls." All of the controls are important; however, Franklin believes that if you had to choose a single control in the top

Resounding Success with Tripwire IP360

The state rolled out its pilot project using Tripwire IP360, a proven VM solution, and has experienced great success in risk reduction. Following the initial deployment, they worked with various state agencies and entities across the state to identify and remediate existing vulnerabilities. At the state level, this allowed them to reduce vulnerability risk by over 50 percent, with one agency reducing its risk by 84 percent.

One of the most valuable—though unanticipated results—of the project has been a notable increase in visibility to the state's IT infrastructure. They use Tripwire IP360 as an inventory and incident response tool as well as a VM solution. With it, the state now knows the number and type of IT assets on its network, satisfying CSC controls 1 and 2. They also know the vulnerabilities on those assets so they can prioritize and quickly remediate them.

This cross-enterprise inventory has proven extremely valuable. For example, when the Heartbleed threat emerged they could immediately find and correct any instances of systems running the affected versions of OpenSSL—a response that previously would have taken much longer and required significant manual effort.

The heightened visibility continues to drive many decisions and changes in mindsets about security across Iowa. For example, they now scan all systems for vulnerabilities prior to deployment.

In addition, the state, its agencies, cities, counties and schools running Tripwire IP360 can now communicate about risk using a common language. Each entity now measures risk using a standardized risk score based on the same metrics. This shared means of measuring and scoring lets them more easily discuss and compare scores across groups. In turn, this drives behavioral changes in ways that address cybersecurity challenges.

Although the initial plans were to deploy the solution to a handful of state agencies, county governments and schools, the deployment quickly grew. Franklin notes, "We just surpassed 100 entities due to the popularity of the product and the project's success."

Concrete Results and Lessons Learned from Using the 20CSC and Tripwire IP360

Through its VM project and recent risk assessment, the State of Iowa learned the value of looking at its security program holistically through the lens of the 20 CSC. State security programs should consider addressing some activities in each control area to build that solid foundation of security. Specifically, by focusing on meeting the bulk of the requirements of the top five controls, any state can dramatically improve its security posture.

Ideally a state could fully address all 20 Controls. However, whether an organization is in the public or private sector, time and resources dictate the need for prioritization. When determining where to start, even within the first five controls, consider which control offers the greatest security improvements. Iowa recommends starting with Control 4, vulnerability management, because it immediately detects and fixes weaknesses that hackers can leverage.

Similarly, Control 3, secure configuration management (SCM) protects systems by ensuring that they're configured securely. Iowa plans to launch its next project around SCM, and expects to experience successes similar to its VM project.