Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Opportunities to Improve Snohomish County's Information Technology Security

August 27, 2020

Report Number: 1026804

Table of Contents

The mission of the State Auditor's Office

Provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective.

The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic **subscription service**.

We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program.

For more information about the State Auditor's Office, visit **www.sao.wa.gov**.

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email **Webmaster@sao.wa.gov** for more information.

State Auditor's Office contacts

State Auditor Pat McCarthy
564-999-0801, **Pat.McCarthy@sao.wa.gov**

Scott Frank – Director of Performance & IT Audit
564-999-0809, **Scott.Frank@sao.wa.gov**

Kelly Collins – Director of Local Audit
564-999-0807, **Kelly.Collins@sao.wa.gov**

Peg Bodin, CISA – Assistant Director of IT Audit
564-999-0965, **Peggy.Bodin@sao.wa.gov**

Kathleen Cooper – Director of Communications
564-999-0800, **Kathleen.Cooper@sao.wa.gov**

To request public records

Public Records Officer
564-999-0918, **PublicRecords@sao.wa.gov**

Introduction

Critical government services depend on information technology systems with confidential information, which must be protected to avoid service disruptions and financial losses

Governments depend on information technology (IT) systems to deliver an array of critical functions. The security of IT systems and related data underpins the stability of government operations, and the safety and well-being of residents. The public expects governments to protect these systems from IT security incidents that could disrupt government services. Delivering on that expectation is paramount to maintaining public confidence.

These IT systems also process and store confidential data. Aside from the loss of public confidence, a data breach involving this information can cause governments to face considerable tangible costs, including those associated with identifying and repairing damaged systems and notifying and helping victims.

IT security incident

Any unplanned or suspected event that could pose a threat to the confidentiality, integrity or availability of information assets.

Data breach

An IT security incident that results in the confirmed disclosure of confidential information to an unauthorized party.

Government IT systems and data are attractive targets for cyberattacks

Government IT systems present a particularly tempting target to cyber criminals. In addition to selling stolen information for financial gain, attackers often target government systems with ransomware, essentially rendering IT systems and data unavailable until the attackers are paid. Because government IT systems support critical operations, attacked governments are often placed in the difficult position of either failing to deliver core services or paying an expensive ransom to the attackers.

Government organizations across the country and around the world have been critically affected by cybercrime. Since 2017, the United Kingdom's National Health Service, the cities of Atlanta and Baltimore, Garfield County in Utah, the Texas judiciary, Texas Department of Transportation and 22 municipalities in Texas, to name a few, have been attacked with ransomware that crippled or disrupted their operations.

Washington governments have also been affected by cyberattacks. Since 2016, nine Washington governments have reported data breaches to the Washington State Attorney General's Office as a result of a cyberattack. Multiple state and local governments have also reported cybersecurity incidents to the State Auditor's Office, including ransomware frauds that occurred as the result of cybersecurity activity.

To help Washington's local governments protect their IT systems, we offer them the opportunity to participate in a performance audit designed to identify opportunities to improve their IT systems.

Snohomish County chose to participate in this audit.

This audit looked for opportunities to improve Snohomish County's information security

To help Snohomish County protect its IT systems and secure the data it needs to operate, we conducted a performance audit designed to identify opportunities to improve IT security. This audit answered the following questions:

- Does the county have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the county's IT security practices align with selected security controls?

Evaluating effective implementation of IT security practices

To determine if the county has implemented effective IT security practices, we conducted tests to determine if selected controls were implemented properly and functioning effectively.

Additionally, our subject matter experts conducted tests on the county's IT systems and ranked the identified weaknesses by the severity and ease in which the identified weakness could be exploited, based on those experts' experience.

Comparing the county's IT security program to leading practices

We assessed the county's IT security policies, procedures and practices against selected leading practices in this area to identify any improvements that could make them stronger. We selected leading practices from the *Controls* issued by the Center for Information Security. The *CIS Controls* were developed by a broad community of private and public sector stakeholders after examining the most common attack patterns. The *Controls* are a prioritized list of control areas designed to help organizations with limited resources optimize their security defense efforts to achieve the highest return on investment.

We gave county management the results of the tests as they were completed.

Next steps

Our performance audits of local government programs and services are reviewed by the local government's legislative body and/or by other committees of the local government whose members wish to consider findings and recommendations on specific topics. Snohomish County's legislative body will hold at least one public hearing to consider the findings of the audit. Please check Snohomish County's website for the exact date, time and location. The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations, and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains more information about our methodology.

Audit Results

The results of our audit work and recommendations were communicated to Snohomish County's management for its review, response and action. We found that, while the county's IT policies and practices partially align with industry leading practices, there are areas where improvements can be made.

Because the public distribution of tests performed and test results could increase the risk to the county, distribution of this information is kept confidential under RCW 42.56.420 (4), and under Generally Accepted Government Auditing Standards, Sections 9.61-9.67. We shared detailed results with the county.

Recommendations

To help ensure Snohomish County protects its IT systems and the information contained in those systems, we make the following recommendations:

- Continue remediating identified gaps
- Revise the county's IT security policies and procedures to align more closely with leading practices

Auditor's Remarks

The Office of the Washington State Auditor recognizes Snohomish County's willingness to volunteer to participate in this audit, demonstrating its dedication to making government work better. It is apparent the county's management and staff want to be accountable to the citizens and good stewards of public resources. Throughout the audit, they fostered a positive and professional working relationship with the State Auditor's Office.

Auditee Response

Snohomish County
Information Technology

3000 Rockefeller Ave., M/S 709
Everett, WA 98201-4046
(425) 388-3703
www.snoco.org

Dave Somers
County Executive

Viggo Forde
Director

August 19, 2020

Peggy Bodin
Assistant Director of IT Audits
Office of the Washington State Auditor
302 Sid Snyder Ave SW
Olympia, WA 98504-0021

Dear Ms. Bodin

On behalf of the Snohomish County Information Technology Department, thank you for the opportunity to review and respond to the cybersecurity performance audit report, "Opportunities to Improve Snohomish County's Information Technology Security."

It was a pleasure working with Michael Hjermstad, Keith Drake, Erin Laska and other State Auditor Staff as well as the subject matter experts who evaluated Snohomish County Information Technology security controls. The engagement with your team was professional and collaborative.

Thank you for recognizing the measures we have taken to protect our technology environment from numerous threats. We appreciate the efforts of those involved to evaluate our information technology security program and the recommended opportunities for improvement. Several of the recommendations have already been put into place to strengthen our IT Security Program. We remain committed to addressing the remaining recommendations in the report and to continuously improve our processes and capabilities.

Sincerely,

Tim Wise
Information Security Officer
Snohomish County Information Technology
3000 Rockefeller Ave
Everett, WA 98201

Appendix A: Initiative 900

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations sections of this report.

I-900 element		Addressed in the audit
1.	Identify cost savings	**No.** The audit did not identify measurable cost savings. However, strengthening IT security could help the county avoid or mitigate costs associated with a data breach.
2.	Identify services that can be reduced or eliminated	**No.** The audit objectives did not address services that could be reduced or eliminated.
3.	Identify programs or services that can be transferred to the private sector	**No.** The audit did not identify programs or services that could be transferred to the private sector.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit compared the county's IT security controls against leading practices and made recommendations to align them.
5.	Assess feasibility of pooling information technology systems within the department	**No.** The audit did not assess the feasibility of pooling information systems; it focused on the county's IT security posture.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit evaluated the roles and functions of IT security at the county and made recommendations to better align them with leading practices.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not identify a need for statutory or regulatory change.
8.	Analyze departmental performance, data performance measures, and self-assessment systems	**Yes.** The audit examined and made recommendations to improve IT security control performance.
9.	Identify relevant best practices	**Yes.** The audit identified and used leading practices published by the Center for Internet Security to assess the county's IT security controls.

Compliance with generally accepted government auditing standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with Generally Accepted Government Auditing Standards (July 2018 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B: Scope, Objectives and Methodology

Scope

The audit assessed the extent to which Snohomish County's IT security programs, including their implementation and documentation, aligned with selected *CIS Controls* and their supporting sub-controls. This audit did not assess the county's alignment with federal or state special data-handling laws or requirements.

Objectives

To help Snohomish County protect its IT systems and secure the data it needs to operate, we conducted a performance audit designed to identify opportunities to improve IT security. This audit answered the following questions:

- Does the county have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the county's IT security practices align with selected security controls?

Methodology

To answer the audit objectives, we conducted technical testing on the county's internal network, and we compared the county's IT security programs to selected leading practices.

External and internal security testing

To determine if the county has vulnerabilities in its IT environment we conducted external and internal security testing of selected key applications, systems and networks. We completed this work in January and February of 2020. This included identifying and assessing vulnerabilities and determining whether they could be exploited.

Comparing the county's IT security programs to leading practices

To determine whether the county's IT security practices align with leading practices, we interviewed key county IT staff, reviewed the county's IT security policies and procedures, observed county security practices and settings, and conducted limited technical analysis of county systems. This work was completed at the county between January and April 2020.

We used selected controls from the *CIS Controls, version 7.1,* as our criteria to assess the county's IT security programs and to identify areas that could be made stronger.

CIS – the Center for Internet Security – is a nonprofit organization focused on safeguarding public and private organizations against cyber threats. Its *CIS Controls* are a prioritized set of leading practices for cyber defense created to stop the most pervasive and dangerous attacks, are informed by analysis of real-world attack data, and are developed and vetted across a broad community of government and industry practitioners. Contributors to the *CIS Controls* have included the U.S. Department of Defense, the National Security Agency, the U.S. Department of Energy national energy labs, law enforcement organizations, Verizon, HP and Symantec.

Each control consists of a series of sub-controls that are distinct and measurable tasks; when the sub-controls are implemented together, they fully meet the requirements of the overall control. We assessed the county against all applicable sub-controls to determine the alignment with each of the overall controls examined. We did this by assessing the extent to which the county met each sub-control in three areas:

1. **Implementing** the sub-control
2. **Automating or technically enforcing** the sub-control, which minimizes the possibility of the sub-control failing due to human error or inconsistent processes
3. **Maintaining documentation** to support the sub-control, such as policies or procedures

We also assessed the extent to which the county's IT management was **reporting** on the control to county leadership.

Work on internal controls

This audit assessed the IT security internal controls at Snohomish County. We used a selection of controls from the 20 *CIS Controls* as the internal control framework for the assessment. The first six are considered among the most important controls to put in place to protect an organization. Based on an initial assessment, we selected four of the top six controls to include in the scope. To protect the county's IT systems, and the confidential and sensitive information in those systems, this report does not identify the specific controls assessed during the audit. We completed our assessment for the purpose of identifying opportunities for the county to improve its internal IT security controls, but not to provide assurance on the county's current IT security posture.