CYBER SECURITY

Special Report 2022

Keeping an independent eye on government IT security

START

Office of the Washington State Auditor
Pat McCarthy

Our work helps state agencies, cities, counties and more improve their cybersecurity posture

The State Auditor's Office plays a distinctive role in Washington's broader cybersecurity landscape. Our independent, customized cybersecurity audits of state agencies and local governments have given us insight into broad security trends facing governments.

< BACK

NEXT >

A message from the State Auditor

Washington's state and local governments possess countless IT systems that provide critical government services and handle vital and sometimes very personal data. They're used to operate numerous programs, touching public safety and prisons, foster care and water systems, financial records and vaccination programs. The public expects government to do all it can to ensure that these systems are secure so critical services can be delivered and data stored in those systems is not lost, stolen or damaged.

Our Office works with state and local governments to help improve their cybersecurity programs through audits and outreach activities. Our staff have invested time and studied extensively to gain expertise in IT auditing and cybersecurity evaluation. SAO's website is stocked with up-to-date resources that local governments can apply to improve their programs even before we conduct an actual audit.

This short overview of our work and findings offers legislators, the public and government leaders information they need to help ensure our state's critical IT systems and data remains protected.

< BACK

NEXT >

Cybersecurity with SAO: A mix of audit and advice

We focus on improvement – moving the needle on IT security for governments large and small

Our team of highly experienced auditors and cybersecurity experts have promoted actionable, achievable solutions through tailored audit recommendations, on-site security consultations and technical presentations. As of December 2021, 60 agencies and local governments have reaped the benefits of our customized audit program.

In addition, we incorporate security topics including patch management, backup and recovery into many of our routine audits, extending our cybersecurity work to hundreds of additional local governments.

Most governments begin making improvements before the audit has even concluded. As for those local governments we have yet to meet, our suite of #BeCyberSmart resources can help them begin their cybersecurity journey.

Our cybersecurity work by the numbers

30 **audits at state agencies**

Representing more than 85% of the state workforce (excluding universities)

30 **audits at local governments**

In 14 counties, on both sides of the Cascades

556 **critical and high vulnerabilities**

identified at state agencies and local governments. These are the most severe vulnerabilities and could be exploited by hackers to cause a security breach

55 **resources to #BeCyberSmart**

48 Audit Connection blog posts and 7 specialized resources in #BeCyberSmart, covering topics from phishing and ransomware to first steps in developing cybersecurity policies

<BACK

NEXT>

Right-sizing our audits is key, because cybersecurity is not "one size fits all"

Large state agency? Small specialty district?

We know the extensive cybersecurity program a big state agency needs to protect sensitive data for thousands of Washingtonians would overwhelm a local government with only a few employees. Our most important goal for each: Improvement, continually moving the needle on IT security

Our staff brings a deep bench of expertise

Between them, our audit staff have built up decades of experience and hold advanced certifications in cybersecurity. We also engage specialists from private firms when an audit needs them.

What's in a cyberauditor's toolkit?

- **Selected elements from the Center for Internet Security's Controls.** The CIS Controls are a prioritized list of security activities designed to help organizations implement IT security controls that provide the biggest bang for their limited dollars.
- **Ethical hacking.** Techniques used during limited penetration testing probe systems for weaknesses that a cybercriminal could leverage to steal data or lock computers for ransom.
- **Conversations.** Some clients are well on their way to a mature cybersecurity program; others are just beginning. Our performance audits evaluate clients' existing practices and identify specific problems and recommendations based on their individual needs.

< BACK

NEXT >

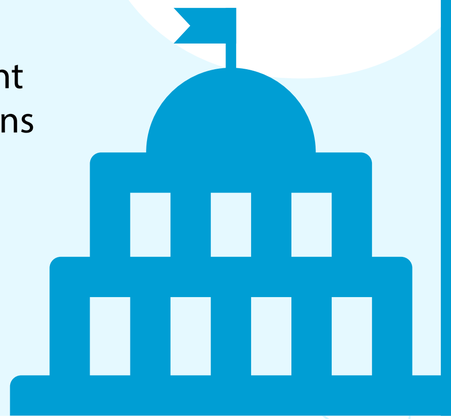
Most audits assess clients' basic cyber hygiene

Leading practices that are the IT equivalent of brushing your teeth

Essential CIS Controls that informed audits at 20 state agencies and 22 local governments

To identify ways our clients can improve their cybersecurity systems and processes, we compare their existing controls with a selection of the CIS "Basic Six" controls. These controls are derived from the most pervasive and dangerous attack patterns and vetted by a broad community of private and public sector stakeholders.

Each control is underpinned by a set of sub-controls that describe precise actions an organization should take to fully enact each goal area. Our assessments use a five-value scale that considers the degree to which a client has implemented each sub-control. Then we offer targeted recommendations that are most likely to help it protect IT systems and data. Armed with this knowledge, our clients can then prioritize actions against their own risks.



The CIS Controls "Basic Six"

1. Inventory and control hardware assets
2. Inventory and control software assets
3. Continuous vulnerability management
4. Control use of administrative privileges
5. Securely configure hardware and software on mobile devices, laptops, workstations and servers
6. Maintain, monitor and analyze audit logs

<BACK

NEXT>

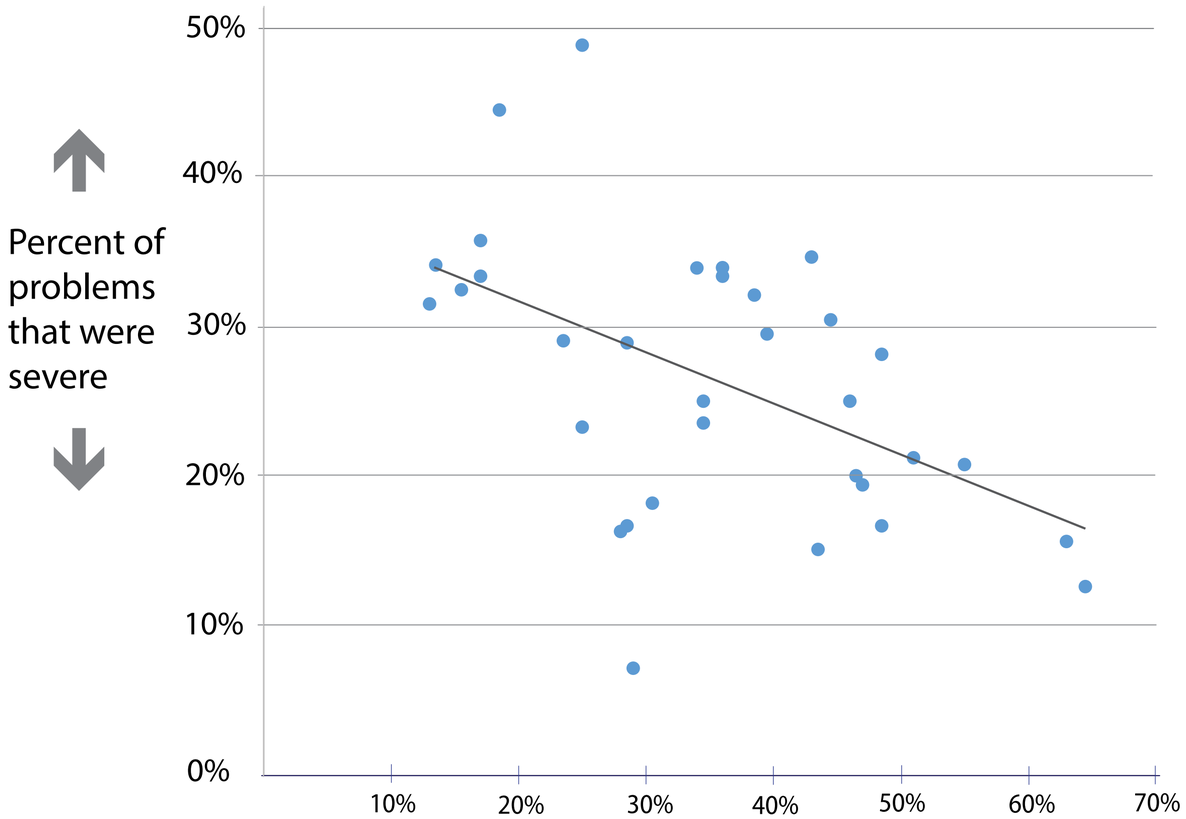
Better controls produce better assessment results

No one is required to follow the CIS leading practices, but we find those who do tend to have less severe vulnerabilities.

33 **state agencies and local governments** have received both a CIS Controls assessment and penetration testing.

Our work found governments that had better practices for managing vulnerabilities and controlling who had access to IT management rights tended to have less severe penetration test results. The graphic shows that correlation between stronger controls and less severe problems.

And that likely means less risk to their systems, too.



< BACK

NEXT >

Tone at the top matters, in all settings

Several common themes appear across many of our audits. The most important: how essential management buy-in is to cybersecurity success.

- **Success starts at the top.** A number of agencies and local governments with particularly strong audit results had leadership that demonstrated their interest in and support for cybersecurity.

  IT managers at those organizations say that their top brass spoke regularly about the importance of cybersecurity to colleagues and staff. Leadership made a point of holding open and regular conversations with IT managers and staff to learn more about security.

- **Without it, even dedicated staff struggle to succeed.** On the other hand, we observed that some governments struggled to implement robust security controls. Here, the IT managers often said they found it hard to get the resources they needed.

  These managers often reported difficulty convincing their government's leadership of the importance of cybersecurity, at least as compared to other priorities. The consequences of under-investment can be severe if a cyber attack succeeds.

< BACK

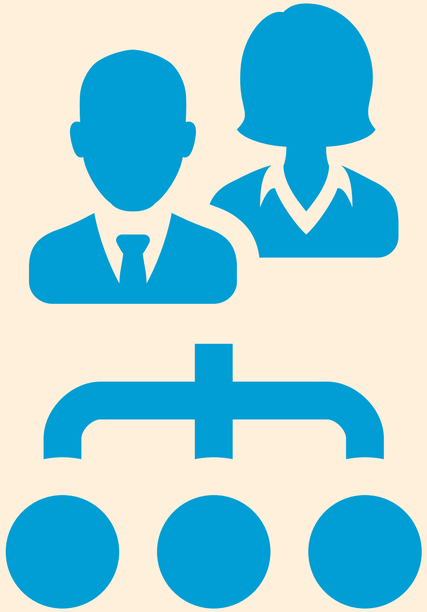
NEXT >

We find that people who do the important work of cybersecurity are in scarce supply

A national shortage of qualified IT and cybersecurity workers is reflected in Washington

Our state is home to many large tech companies, able and willing to pay top wages to their recruits. This poses unique challenges for state and local governments in hiring and retaining highly qualified IT staff.

State agencies and local governments often report they have problems with having enough staff. This includes having sufficient resources for staff, as well as finding appropriately trained or qualified IT-security employees. Among state agencies, staff often leave one position to work at another agency. While this often benefits the employee and the new employer, this does not offer the state the benefit of bringing more IT expertise into public service or consistency to the organization.



What can the state do about it?

https://schoolchoices.org/index.php?/colleges/in/washington/field/5

As of December 2021, more than 50 colleges and universities offered computer science and IT degree programs, including 38 public schools. Supporting these programs can help build a pipeline of workers with the training and skills Washington will need to support its cybersecurity goals at every level of local and state government.

<BACK

NEXT>

We work with three partner agencies

The possibility of a catastrophic cyber event occurring in Washington is an ever-present threat. Preparing for and responding to cyber incidents is not the responsibility of any single office or department. It requires continuous collaboration across multiple agencies.

Three state agencies have primary responsibility for preventing, detecting or responding to cybersecurity incidents.

The State Auditor's role is unique.

Because we do not set IT security policies, or supply IT hardware, software or services, we are able to provide an independent review of cybersecurity practices for both state and local government bodies.

Washington Technology Solutions (WaTech)

State's primary technology agency, responsible for state-level cybersecurity, including incident response

Military Department

Governor's homeland security advisor, responsible for helping secure critical infrastructure and coordinating statewide emergency responses

Secretary of State's Office

Responsible for elections, protects the statewide Election Management System and the state's Voter Registration database

State Auditor's Office

Conducts independent cybersecurity audits of state agencies and local governments, provides cybersecurity resources for local governments, plus trainings, presentations and consultations

< BACK

NEXT >

Continuing cybersecurity work in 2022 and beyond

Streamline internal processes to maximize our own resources

Our cybersecurity specialists and IT auditors lend their expertise to a wide variety of audits, including fraud and accountability work. We actively seek to improve our own processes in data handling, reporting and time management to ensure we make best use of our time and money.

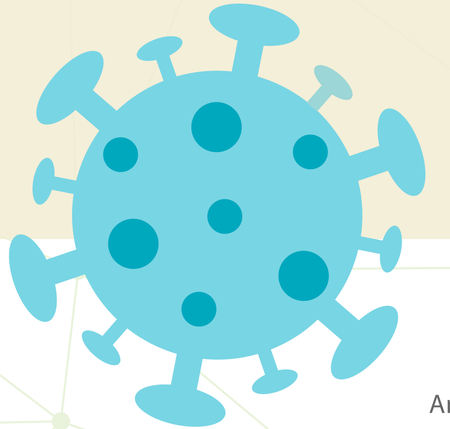
Provide information that empowers our clients to make sound choices in protecting their IT systems

Our expertise in cybersecurity auditing is most valuable when we share our knowledge with our clients. We provide:

- Guidance in adopting voluntary cybersecurity frameworks like the CIS Controls
- Online resources that offer local governments actionable starting points
- Independent assessments at state agencies that include leading practices that can strengthen their compliance with IT security requirements

Continuing audits during the pandemic

We made the move to remote auditing in March 2020. Overall, we have found the transition to be successful and sustainable for the foreseeable future. However, we have noticed that audits sometimes take a little longer in this environment. In adapting to auditing in a remote environment, flexibility and robust communication have been key to performing timely audits.



< BACK

NEXT >

Want to know more? Just ask us!

Phone: 564-999-0950

TDD Relay: 800-833-6388

For information about how to request a cybersecurity audit, please call Erin Laska, Audit Manager, at 1 360-594-0615.

How to print this report:

- Move your mouse curser to the bottom of your browser window. A bar will appear with several icons. Click the "download PDF" button.
- Open the downloaded PDF, and choose the "print" option from your PDF reader.
- Be sure to check "landscape" orientation and, if possible, at least legal-sized paper for better ease of reading.
- Consider "printing on both sides, flip on short edge" to save paper.
- Finally, decide whether you want full color or grayscale – we know folks rooted in #GoodGovernment are judicious with printer ink.