Office of the Washington State Auditor
Pat McCarthy

Continued Cybersecurity Efforts at the State Auditor's Office

Joint Legislative Audit and Review Committee

Erin Laska, *IT Security Audit Manager*
Clyde-Emmanuel Meador, *IT Auditor*

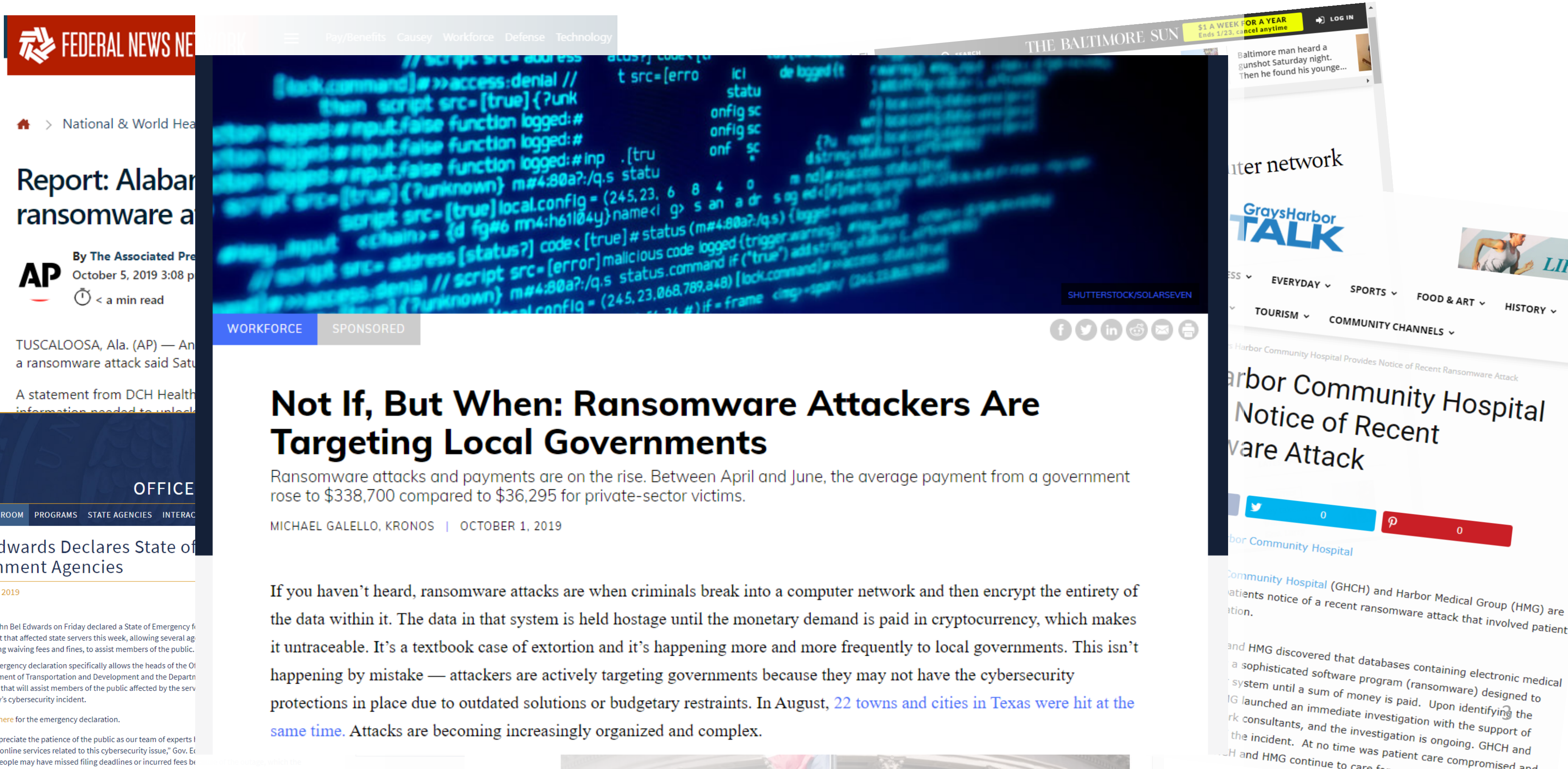
February 5, 2020

Roadmap for today’s presentation

- Current threats to state and local governments
- Cyber-related illegal activities reported to the State Auditor
- Cybersecurity performance audits
- Other cybersecurity assistance
- 2019 State Cybersecurity presentation

Cybersecurity poses a risk, nationally and in Washington

Ransomware is on the rise, targeting state and local governments



FEDERAL NEWS NETWORK

Pay/Benefits Causey Workforce Defense Technology

National & World Hea

Report: Alabar ransomware a

By The Associated Pre

October 5, 2019 3:08 p

< a min read

TUSCALOOSA, Ala. (AP) — An a ransomware attack said Satu

A statement from DCH Health information needed to unlock

OFFICE

ABOUT NEWSROOM PROGRAMS STATE AGENCIES INTERAC

Gov. Edwards Declares State of Government Agencies

November 22, 2019

Gov. John Bel Edwards on Friday declared a State of Emergency f incident that affected state servers this week, allowing several ag including waiving fees and fines, to assist members of the public.

The emergency declaration specifically allows the heads of the Of Department of Transportation and Development and the Departm actions that will assist members of the public affected by the serv Monday's cybersecurity incident.

- Click here for the emergency declaration.

"We appreciate the patience of the public as our team of experts restore online services related to this cybersecurity issue," Gov. Ed some people may have missed filing deadlines or incurred fees be

SHUTTERSTOCK/SOLARSEVEN

WORKFORCE SPONSORED

Not If, But When: Ransomware Attackers Are Targeting Local Governments

Ransomware attacks and payments are on the rise. Between April and June, the average payment from a government rose to $338,700 compared to $36,295 for private-sector victims.

MICHAEL GALELLO, KRONOS | OCTOBER 1, 2019

If you haven't heard, ransomware attacks are when criminals break into a computer network and then encrypt the entirety of the data within it. The data in that system is held hostage until the monetary demand is paid in cryptocurrency, which makes it untraceable. It's a textbook case of extortion and it's happening more and more frequently to local governments. This isn't happening by mistake — attackers are actively targeting governments because they may not have the cybersecurity protections in place due to outdated solutions or budgetary restraints. In August, 22 towns and cities in Texas were hit at the same time. Attacks are becoming increasingly organized and complex.

THE BALTIMORE SUN

$1 A WEEK FOR A YEAR Ends 1/23, cancel anytime

LOG IN

Baltimore man heard a gunshot Saturday night. Then he found his younge...

ıter network

GraysHarbor TALK

EVERYDAY SPORTS FOOD & ART HISTORY

TOURISM COMMUNITY CHANNELS

s Harbor Community Hospital Provides Notice of Recent Ransomware Attack

ırbor Community Hospital Notice of Recent ware Attack

0 0

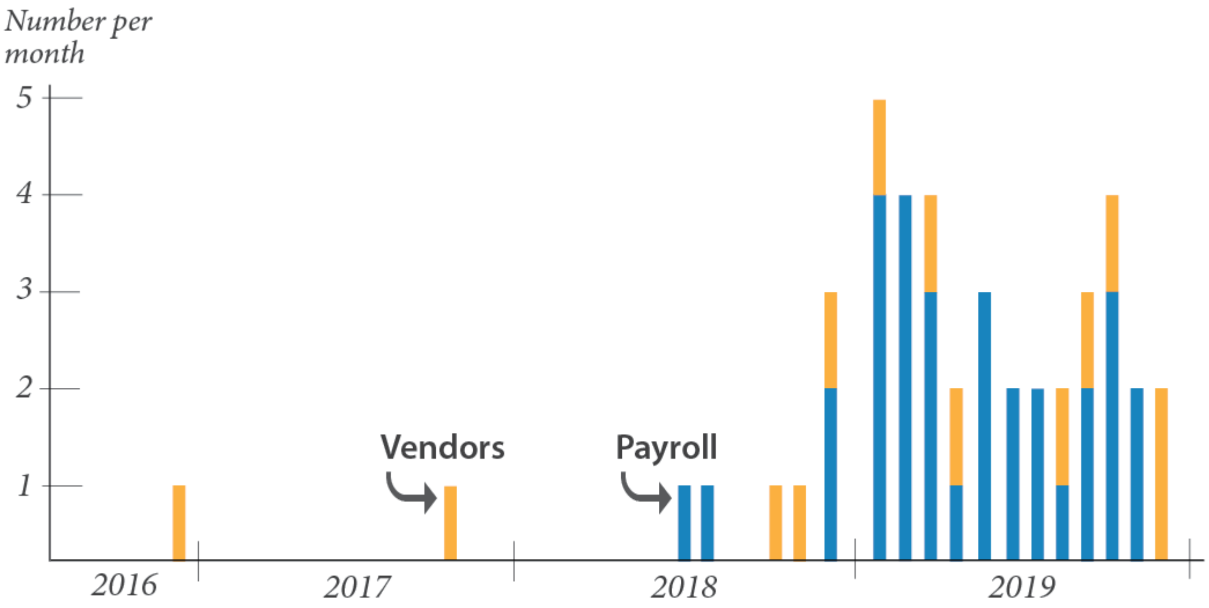
rbor Community Hospital

Community Hospital (GHCH) and Harbor Medical Group (HMG) are patients notice of a recent ransomware attack that involved patient ation.

and HMG discovered that databases containing electronic medical a sophisticated software program (ransomware) designed to system until a sum of money is paid. Upon identifying the IG launched an immediate investigation with the support of rk consultants, and the investigation is ongoing. GHCH and the incident. At no time was patient care compromised and H and HMG continue to care fo

Phishing attacks – also on the rise – put automated banking transactions at risk

Automated Clearing House (ACH) frauds on the rise

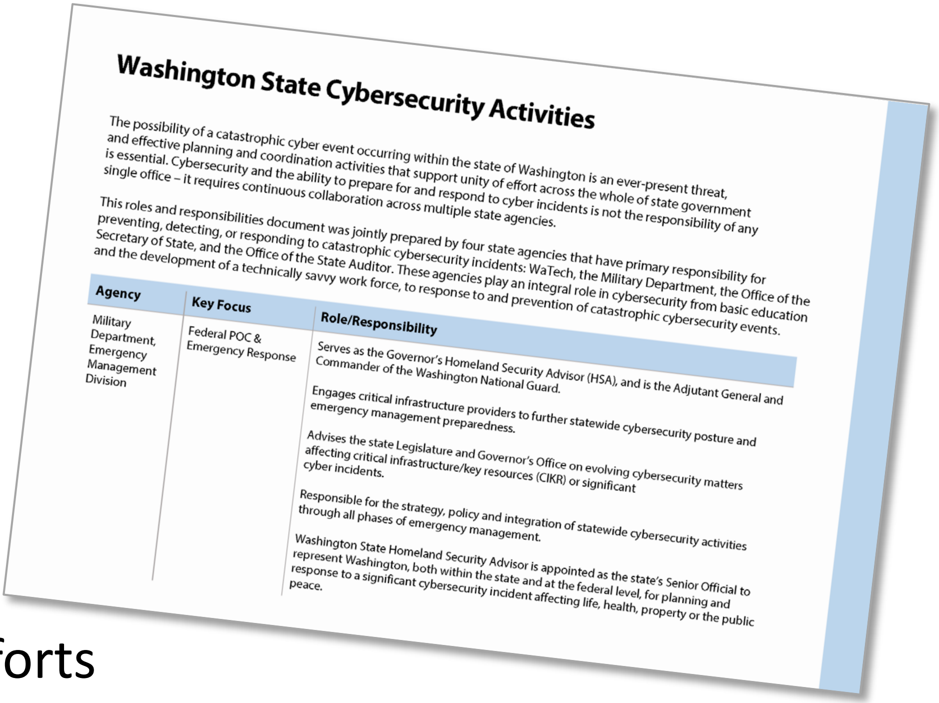


State law requires all state agencies and local governments to notify us immediately about known or suspected loss of public resources

Many stakeholders in Washington's cybersecurity efforts

They include:

- WaTech's Office of the Chief Information Officer and Office of Cybersecurity
- Military Department's Emergency Management Division
- Secretary of State's Office



Washington State Cybersecurity Activities

The possibility of a catastrophic cyber event occurring within the state of Washington is an ever-present threat, and effective planning and coordination activities that support unity of effort across the whole of state government is essential. Cybersecurity and the ability to prepare for and respond to cyber incidents is not the responsibility of any single office – it requires continuous collaboration across multiple state agencies.

This roles and responsibilities document was jointly prepared by four state agencies that have primary responsibility for preventing, detecting, or responding to catastrophic cybersecurity incidents: WaTech, the Military Department, the Office of the Secretary of State, and the Office of the State Auditor. These agencies play an integral role in cybersecurity from basic education and the development of a technically savvy work force, to response to and prevention of catastrophic cybersecurity events.

Agency	Key Focus	Role/Responsibility
Military Department, Emergency Management Division	Federal POC & Emergency Response	Serves as the Governor's Homeland Security Advisor (HSA), and is the Adjutant General and Commander of the Washington National Guard. Engages critical infrastructure providers to further statewide cybersecurity posture and emergency management preparedness. Advises the state Legislature and Governor's Office on evolving cybersecurity matters affecting critical infrastructure/key resources (CIKR) or significant cyber incidents. Responsible for the strategy, policy and integration of statewide cybersecurity activities through all phases of emergency management. Washington State Homeland Security Advisor is appointed as the state's Senior Official to represent Washington, both within the state and at the federal level, for planning and response to a significant cybersecurity incident affecting life, health, property or the public peace.

We focus our work in areas that do not overlap with other efforts

Overview of cybersecurity audits

Cybersecurity performance audits

- ✓ State agencies
- ✓ Local governments

Related performance audits

- ✓ 2018 Contract Assurances for Vendor-Hosted State IT Applications
- ✓ 2014 & 2018 Safe Data Disposal
- ✓ 2020 Data and System Backup and Disaster Recovery

#BeCyberSmart Campaign

- Curated suite of cybersecurity resources for local government
- Customized by role in government
- Designed as a place for governments to start

www.sao.wa.gov/becybersmart/

Opportunities To Improve State IT Security – 2019

Cybersecurity is important, so we audit it

- IT security affects everyone
  - ✓ Critical services
  - ✓ Data breaches

- State agencies must protect their systems and data

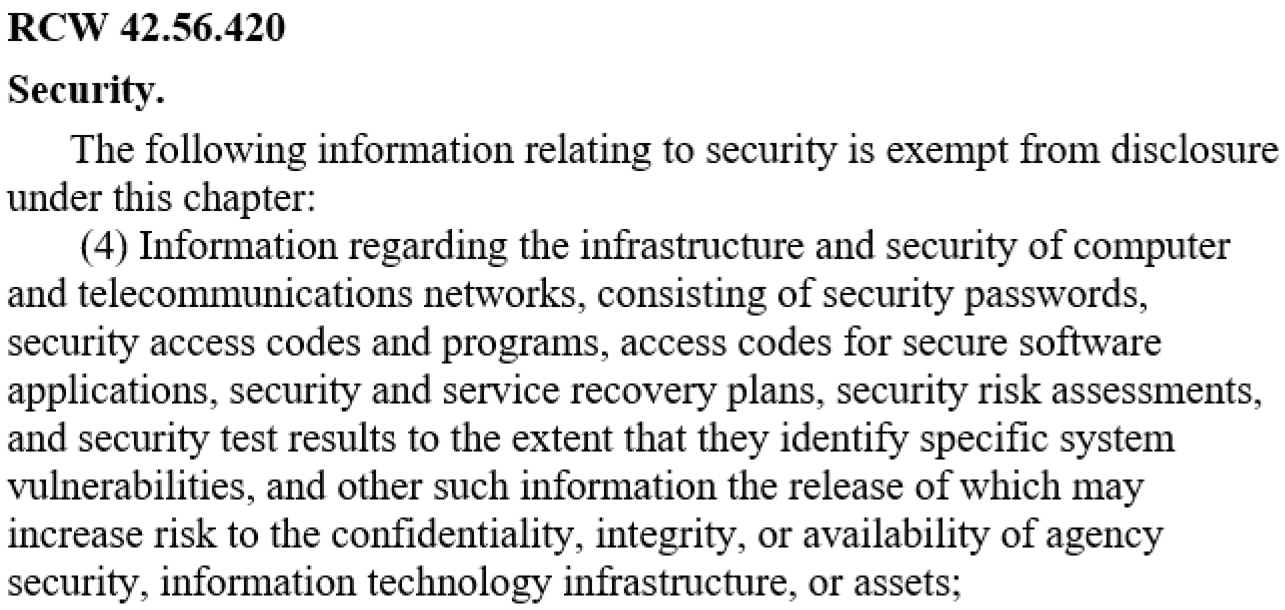
- Because of this, we looked for opportunities for agencies to improve their IT security and related practices

Audit overview – Cyber 5

- 2019 cybersecurity performance audit of selected state agencies
  - ✓ Three large agencies and one small agency
- Fifth in this series of audits, covering 17 agencies
- Assessed network and application security and IT security practices

Protecting sensitive information

Confidentiality is key



RCW 42.56.420

Security.

The following information relating to security is exempt from disclosure under this chapter:

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets;

Our audit asked

Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

Can selected agencies make their IT systems more secure?

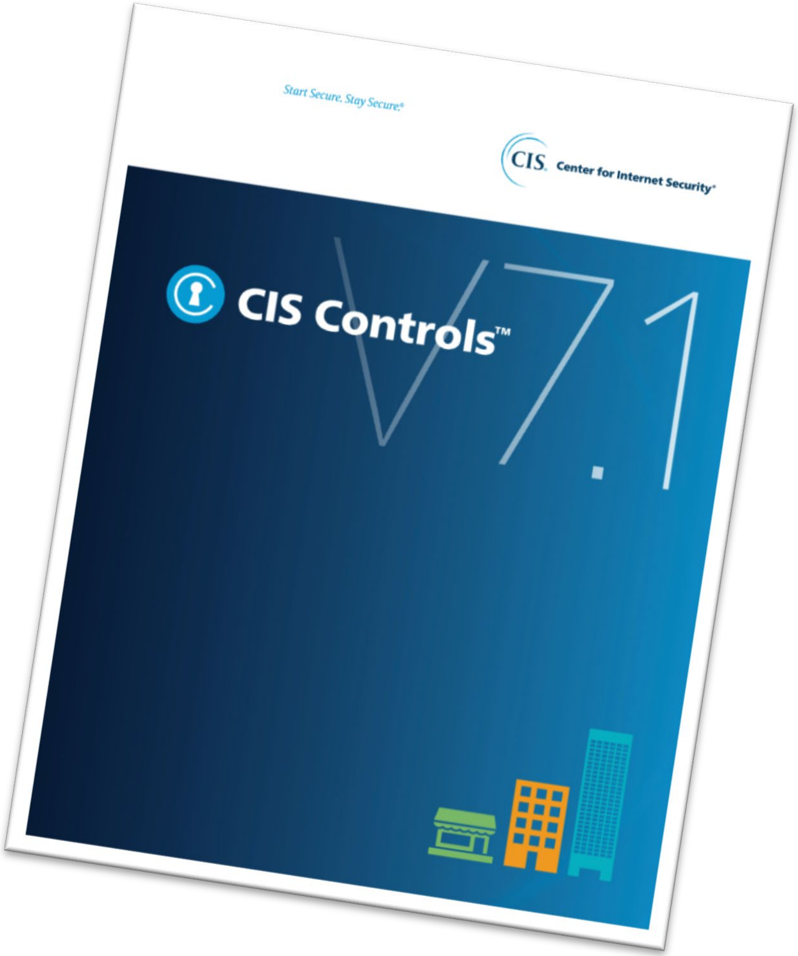
- Penetration testing of each agency’s network and applications
  - ✓ External
  - ✓ Internal
- Performed by contracted subject matter experts

Can they better align their IT security practices with leading practices?

- Compared agency practices to controls from the Center for Internet Security

  ✓ Informed by private- and public-sector stakeholders

  ✓ Prioritize benefits



Start Secure. Stay Secure.®

CIS. Center for Internet Security®

CIS Controls™

V7.1

The CIS Controls we used

CIS “basic controls”

1. Inventory and control of hardware assets
2. Inventory and control of software assets
3. Continuous vulnerability management
4. Controlled use of administrative privileges
5. Secure configurations for hardware and software
6. Maintenance, monitoring and analysis of audit logs

plus

7. Email and web browser protections

11. Secure configurations for network devices

Results overview

- We found strengths in agencies’ security, but also areas where agencies can improve security by:
  - ✓ Remediating vulnerabilities
  - ✓ Improving the way they implement and document controls
- Agencies could use the CIS Controls to improve security
  - ✓ Greater alignment with Controls associated with better penetration testing results

Factors that contributed to performance results

- Agency personnel reported resource constraints, including insufficient personnel, as a challenge

- Agencies that performed better cited high levels of executive involvement and support

- Agencies with higher IT staffing levels performed better than agencies with lower IT staffing levels

Recommendations

We recommend the four state agencies:

- Continue remediating vulnerabilities identified during security testing, starting with those that most significantly affect the agencies
- Identify and continue to periodically assess IT security needs and resources, including personnel and technology
- Consider further aligning agency IT security controls with leading practices recommended in the CIS Controls

Contact Information

Pat McCarthy

State Auditor

Pat.McCarthy@sao.wa.gov

(564) 999-0801

Scott Frank

Director of Performance & IT Audit

Scott.Frank@sao.wa.gov

(564) 999-0809

Erin Laska

IT Security Audit Manager

Erin.Laska@sao.wa.gov

(564) 999-0970

Clyde-Emmanuel Meador

IT Auditor

Clyde-Emmanuel.Meador@sao.wa.gov

(564) 999-0971

Website: www.sao.wa.gov

Twitter: www.twitter.com/WaStateAuditor

Facebook: www.facebook.com/WaStateAuditorsOffice