Experiencing a Security Audit

MIKE ROHRBACH, DIRECTOR, LEG-TECH, WASHINGTON STATE LEGISLATURE

NCSL SUMMIT 2016
## A Bit of Background

### Washington State Legislature

- 49 Senators, 98 Representatives
- 600-700 permanent staff (about 1200-1300 during session)
- Four legislators sit on the governing committee overseeing legislative IT
- Chief Clerk, Secretary of the Senate, and their deputies manage legislative IT
- Representatives from legislative workgroups make recommendations and monitor IT needs, plans, priorities, and performance

### LEG-TECH

- 46 people in LEG-TECH handling infrastructure, communications, security, customer support, training, custom applications
  - Operating systems, servers, networks, email environment, voice mail, phones, web sites, security, identity management, PCs and tablets supported by 12 staff in Technical Support Group
  - Custom applications supported by 18 staff in the Applications Support Group (nearly 300 apps)
  - Front-line customer support, Help Desk, classroom training, documentation, deployment of PCs and tablets, floor support when they’re in session supported by 14 staff in Customer Support Group
Members of the oversight committee offered legislation in the last biennium about cybersecurity incidents, crimes, training
Office of the Chief Information Officer
OCIO Policy 141.10 outlines the security standards for state agencies
Security one of the strategic elements for selecting IT projects
Legislature must have a comparable security program, according to RCW 43.105.215

(1) The office shall establish security standards and policies to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure. The director shall appoint a state chief information security officer. Each state agency, institution of higher education, the legislature, and the judiciary must develop an information technology security program.

(2) Each state agency information technology security program must adhere to the office's security standards and policies. Each state agency must review and update its program annually and certify to the office that its program is in compliance with the office's security standards and policies. The office shall require a state agency to obtain an independent compliance audit of its information technology security program and controls at least once every three years to determine whether the state agency’s information technology security program is in compliance with the standards and policies established by the agency and that security controls identified by the state agency in its security program are operating efficiently.

(3) In the case of institutions of higher education, the judiciary, and the legislature, each information technology security program must be comparable to the intended outcomes of the office's security standards and policies.
Documenting Our Security Program

LEG-TECH has had some security documentation, processes, and an incident response plan in place.

Because legislators are interested and we use state resources, we wanted to improve our program sooner rather than later.

To protect 963 databases, 279 custom applications and services, 181 servers, and 37 virtual networks.

The framework provided by the National Institute of Standards and Technology (NIST) has become the standard for federal, state, and local government, so we decided to build our program around the NIST controls, with an eye toward the OCIO policy.

- Estimate that it took us 1000 hours to set up the framework and documents (one-time cost)
How We Did It

Engaged Myers and Stauffer of Austin
- State resources booked and unfamiliar with NIST
- Myers and Stauffer familiar with state IT in Washington, NIST, and OCIO policy

Team effort
- Core team of 8 people
- 1 point person; 3 infrastructure; 2 app development, 2 customer support

They audited our documentation and infrastructure
- 3.5 months to review documents and infrastructure, conduct phone and web conferences, visit us on site, test the infrastructure, penetration testing, and produce draft and final reports
- 550 hours of LEG-TECH staff time
- 250 documents – used a SharePoint Online site that LEG-TECH and M&S could use
- $40,000 for the engagement
- Plus one-time 1,000 hour initial investment
Results

Our documentation and processes need further work

Legislature needs to address security training for all staff and members

Although we don’t have a lot of it, the Legislature must take steps to further protect the personally identifiable information we do have

Need to make sure that we have all the information on hand to respond to a cyber-security incident and that people know what is in the incident response plan

Infrastructure is secure and we could address many issues as audit was unfolding
Next Steps

Report to legislative leadership mid-August

Work with legislative leadership to execute on priorities for 2016 and make policy decisions

Start process of annual review of documents – estimate 50 hours per month the first year

Consider requirements for cyber-security staffing

Continuously improve our security program, with an eye to the next audit, scheduled for 2019