SENATE FINANCE COMMITTEE
April 26, 2022
9:19 a.m.

9:19:56 AM

CALL TO ORDER

Co-Chair Stedman called the Senate Finance Committee meeting to order at 9:19 a.m.

MEMBERS PRESENT

Senator Click Bishop, Co-Chair
Senator Bert Stedman, Co-Chair
Senator Lyman Hoffman
Senator Donny Olson
Senator Natasha von Imhof
Senator Bill Wielechowski
Senator David Wilson

MEMBERS ABSENT

None

ALSO PRESENT

Bill Smith, Chief Information Officer and Director, Office of Information Technology, Department of Administration.

SUMMARY

^PRESENTATION: CYBER SECURITY

9:20:40 AM

Co-Chair Stedman relayed that the committee would hear a presentation on Cyber Security, and would discuss the administrations associated FY 23 request, which was sprinkled throughout the budget.

9:21:44 AM

BILL SMITH, CHIEF INFORMATION OFFICER AND DIRECTOR, OFFICE OF INFORMATION TECHNOLOGY, DEPARTMENT OF ADMINISTRATION, introduced himself. He thought cyber security was a popular topic on a global level. He described that within the

Office of Information Technology (OIT), cyber security oversight was housed in the state Information Security Office, which had oversight of Cyber Security for the executive branch. He cited that cyber security was the office's top IT priority and was woven throughout the Enterprise Systems. He qualified that his office worked closely with IT leadership in the legislative branch and with the Courts to ensure there was a unified picture.

Mr. Smith discussed a Presentation, "State of Alaska Cyber Security; Presentation to (S) Finance Committee; Bill Smith, Office of Information Technology; 4/26/2022" (copy on file). He turned to slide 2, "Agenda":

Cyber Threat Landscape
Cyber Security Incident Cost
FY23 Cyber Security Requests
Cyber Security Ecosystem
- People
- Technology
- Processes

Questions

Mr. Smith addressed the info-graphic on the slide and explained that it illustrated a framework for considering cyber security. The graphic was generated by the National Institute of Standards in Technology and showed how the cyber security systems and office were organized to reduce risk.

9:24:04 AM

Mr. Smith showed slide 3, "Cyber Threat Landscape":

Threat activity drivers:
- Cybercrime is a $6 trillion annual industry (Security Magazine, 2021)
- Industrialization and automation of cyberattack capabilities
- Nation state threats
- Supply chain activity
- Pre-existing vulnerabilities

Breaches are no longer just a technical problem...threat awareness is the responsibility of the whole organization. (Gartner, 2021)

Mr. Smith referenced an article that had indicated that it was possible to contract a cyber-attack for $200. He discussed the geopolitical aspect of cyber-attacks, through which individuals endeavored to intrude for information in order to influence public opinion. He cited that in 2021 the state had 87 million malicious emails blocked in the executive branch. There were several that had gotten through and had been dealt with. He cited that the systems had captured about 8 billion systems attacks per month over the course of 2021.

Mr. Smith contended that Cyber Security was no longer merely an IT issue, but rather an issue for the whole organization. He asserted that every person had a role in the matter.

9:27:03 AM

Senator Wielechowski noted that in the last couple of years there had been attacks on the Division of Elections and the Department of Health and Human Services. He wondered if there had been other attacks on the state's computer systems.

Mr. Smith mentioned a cyber-attack that got into the state environment before being eradicated. He did not want to share a great deal of detail without the committee being in Executive Session. He relayed that any incident where information was exposed was required by law to be reported. He discussed tracking the range of exposures from a lost laptop to a cyber-attack.

Senator Wielechowski asked if any of the attacks had made demands on the state for money.

Mr. Smith was not aware of any monetary demands as part of the attacks. He thought ransomware was getting the most attention in the press. He cited that about ten percent of the cyber-attacks reported globally were some sort of ransomware. He noted that ransomware was most commonly identified before it came to fruition.

Co-Chair Bishop asked Mr. Smith to repeat the comment about 8 billion attacks.

Mr. Smith restated that over the course of 2021, the state had an average of 8 billion network-based attacks blocked

per month. He qualified that there had been a wide range of attacks that included targeted attacks against state assets as well as others. He mentioned "spray attacks," which included a threat actor sending out automated attacks that pinged every address on the web to find vulnerability.

9:30:23 AM

Mr. Smith referenced slide 4, "Cyber Security Incident Cost" which showed a line graph entitled 'Average total cost of a date breach,' which was measured in millions. He relayed that the global average cost for a data breach was about $4.2 million. The cost was higher in the United States with an average of $9 million. The cost could be impacted by the industry and type of attack. Public sector organizations were typically showing an average of $2 million per incident, which did not include lost business. The cost for private entities included lost business. There was a significant cost for breaches, and the department had seen about a 10 percent increase in cost.

Mr. Smith noted that the cost of cyber security incident costs varied significantly, but provided insight for mitigating potential costs to the state. He noted that the organizations that had high compliance requirements and dealt with a great deal of personal information had higher costs for incidents. He added that ransomware created a higher cost per incident. He relayed that he would discuss preventive measures the state was taking to reduce cost.

Senator Wilson considered the supplemental cost of the budget to address the past years cyber-attacks. He asked if the department had looked into the cost-benefit of cyber security insurance.

Mr. Smith affirmed that the division had looked at cyber security insurance with the resource management division. He thought that cyber security insurance was not a good option for the state and pointed out that insurance did nothing to prevent attacks but did help with financial concerns on the other end. He mentioned that the actuarial tables around cyber security had been skewed by the proliferation of attacks and had not recovered. He shared that several policies had omitted ransomware, and some had deductibles that were as much as 25 percent to 50 percent of the insured amount. He noted that the state was pursuing

an internal path working with the Division of Risk Management on cyber security insurance.

9:33:51 AM

Senator Wielechowski asked if any state actors had been identified in attacking state computer systems.

Mr. Smith stated that he had seen state actors that had been associated with various nation-states all over the globe in activity coming towards Alaska. He noted that very few had been identified in targeted attacks. Many nation-states' individuals from the Ukraine and Russia area had been identified in non-targeted attacks, as well as individuals from other areas. He noted he had more information he could share in an executive session.

Senator Wielechowski asked if Mr. Smith could discuss the breach to the Division of Elections, including who was responsible and what information was obtained.

Mr. Smith did not have details about the breach but knew that the attack would fall into the category of a supply-chain attack, which was one of the categories of attack in which threat actors tried to infiltrate the code of applications to sell to various organizations. He shared that the type of attack was one reason why organizations tried to do good code review. He continued that there was some movement in the cyber security environment to help defend against such attacks.

Senator Wielechowski asked if there had been any attempt to change the election outcome.

Mr. Smith stated, "not to my knowledge."

Senator Wielechowski thought Alaskans were concerned about attempts to change election outcomes. He asked Mr. Smith about his level of confidence regarding the security of election data.

Mr. Smith was very confident in the work his division did to protect the integrity of elections. He recounted that over the course of the previous year there had specific targeted assessments/audits working with the Center for Information Security and Analysis (CISA), which was part of the United States Department of Homeland Security. He

continued that CISA had come and looked at the state's systems, did penetration testing in the state's environments, and worked with the Division of Elections. He elaborated that the division had spent a lot of time on elections as well as the fidelity of the network and looking for vulnerabilities to mitigate. After the work that was done, he was very confident about the level of integrity of the state's elections, based on a cyber-security posture at the Division of Elections.

9:37:32 AM

Mr. Smith advanced to slide 5, "FY23 Budget Cyber Security Requests":

- DOA Azure Adoption to Assist with Cloud Migration – $23,116.0–Obtain professional assistance with State of Alaska migration to the Cloud.

- DOA Microsoft Security Upgrade –$1,149.0–Complete implementation of upgraded State Microsoft licensing to better protect employee accounts and data, reduce security expenditures, and allow the State of Alaska to meet common compliance standards.

- DOA Initiate a 24/7 Security Monitoring Center and Improve Threat Hunting Capabilities –$1,700.0 –Obtain managed 24/7 Security Operations Center (SOC) coverage for a period of 24 months, evaluate SOC requirements for the State to determine enduring requirements and best path forward, and implement internal and/or external capabilities to meet documented cybersecurity requirements.

- DMVA Homeland Security State and Local Cybersecurity Grant Program -IIJA Division J, Title VI -$2,404.4

- DOH Information Technology Security Program Assessment -$1,900.0

Mr. Smith detailed that the bottom two bullets on the slide identified items that applied to other departments.

Senator Wielechowski asked about the process by which the division put out the proposals. He asked if there was a Request for Proposal (RFP) process, and how the process might provide the highest level of security.

Mr. Smith affirmed that the state used a competitive process for proposals. He explained that quite often the division utilized tools from the National Association of State Procurement Officer (NASPO), which included a competitive process. There were standing programs that had been competitively assessed and awarded, which the state could leverage as signatories in the process. The process allowed the state to rapidly find competitively sourced vendors. He discussed selection of vendors, and noted that that the division looked for integration and experience existing systems. He asserted that diverse systems created gaps and areas of potential for vulnerabilities. He cited that the two vendors within DOA had gone through the NASPO process.

9:40:54 AM

Senator Wilson thought the state was approaching cyber-security in a "hodge podge" way. He asked about the plan to cover all its sensitive data when all the departments were not integrated into OIT.

Mr. Smith emphasized the key point that consolidation of IT was one of the critical pillars of strengthening the state's cyber security. He asserted it was very important to have a unified view of cyber security throughout the executive branch.

Senator Wilson thought the current year's budget request was about $26 million. He asked if there had been a statewide assessment or audit to identify security needs and ensure the best process was being employed. He suggested doing an assessment in conjunction with the cloud migration.

Mr. Smith relayed that there had not been a complete cyber security focused assessment, but stated that during the Apex Project, the division had brought in external partners to assess the IT environment across the state and had addressed some aspects of cyber security. The process had also examined the cloud migration path and potential impact. The division had not had a specific cyber security audit in his tenure with the state. He highlighted that there was a new chief information security officer that began in the end of the last year, and an assessment was one of the priorities along with making sure any efforts

were towards increasing security the fastest. He acknowledged that the external audits were extremely valuable but required a great deal of time and effort to complete and would need to be sequenced.

9:43:57 AM

Senator Wilson recalled that data had been breached in other departments in the past two years and thought some of the data could be being used to harm the state. He asked what the state was doing to validate the data that had been stolen and wondered what was being done to secure the systems being used.

Mr. Smith shared that he looked at the issue as larger than what data may have gone out. Because of the prevalence of identity theft and breaches in the environment, the state had to assume compromised data was around at all times. He mentioned multi-factor authentication and other "zero trust" elements being integrated in the state employee environment. He shared that for external areas, the division was focused on anti-fraud and identity verification abilities. He mentioned the success of new capabilities in the MyAlaska platform to combat automated fraud and bots trying to gain access into the environment. He referenced millions of attempted logins to MyAlaska.com, which had shut down services, which was later remedied by a new platform. He summarized that the two primary areas that the state was focused on were the cyber security measures and anti-fraud elements that were being put into place.

Senator Wielechowski asked about larger breaches to DHSS and the Permanent Fund Dividend (PFD) Division, where people's data was compromised. He asked if the administration had complied with the notification requirements to Alaskans regarding the data breach.

Mr. Smith stated that to his knowledge, the administration had complied with the notification requirements. He noted that in the case of a data breach, the IT group solely focused on the incident and how to contain or eradicate it from the state's technical systems. He mentioned business owners and government agencies in relation to reporting requirements and notification schedules.

Senator Wielechowski asked if the administration had been subject to any lawsuits because of identity theft in the last few years.

Mr. Smith was not aware of any such lawsuits.

Senator Wielechowski asked if the administration had provided any remedies for individuals whose identity or information had been stolen.

Mr. Smith did not have first-hand knowledge of what Senator Wielechowski was asking. He thought the matter had been discussed and that it was part of the remediation for business owners of data that had been compromised.

9:48:37 AM

Senator Wilson referenced a hearing about cyber security in the Senate Health and Social Services Committee, in which he had heard that the PFD Division's data was used to notify all Alaskans that they were at risk. He asked about providing all Alaskans with remediation.

Mr. Smith explained that the potential pool of individuals that needed to be notified went through the system that was compromised, and the event was handled and identified by DHSS. He did not have any specific information to offer.

Senator Wilson thought that the data involved any person that went through public assistance and public benefits. He suggested contacting the department to understand the cost of remediation.

Mr. Smith spoke to slide 6, "Cyber Security Ecosystem":

> Cyber security throughout the Information Technology environment:
>
> •People-Staff training that creates a culture of security awareness (Annual cyber training)
>
> •Technology
>
> •Network architecture (Cloud Migration)
>
> •Constantly evolving systems (Security Projects)

- Processes-Organization to support compliance and incident response (IT Consolidation)

Mr. Smith discussed upcoming initiation of a routine monthly test with phishing emails to test effectiveness of employee training.

9:51:38 AM

Mr. Smith addressed slide 7, "Technology -Cloud Migration":

Cyber security benefits of cloud migration:

- Shared Security
  - Provider secures infrastructure
  - We focus on account and access security
- Secure Foundation
  - Modern, continuously updated infrastructure
  - Distributed Denial of Service (DDoS)resistant
- Built-in security controls
  - Managed identity and access
  - Always on encryption (data at rest/in transit)
- Global threat intelligence

Mr. Smith commented that the current network design was developed over decades over a very decentralized government and had many silos. He discussed aging systems and asserted that cloud migration was the most rapid cost-effective path to mitigate risk. He highlighted that the graphic on the right was to show the difference between on-premises and in the cloud. The graphic showed types of cloud computing. The left-hand side of the graphic showed the areas the cloud helped with security. He discussed vendors, which ensured hardware was compliant and saved the state resources. He discussed cloud-based email, which was continually patched with upgrades. The on-premises environment required state employees to manually acquire the patch and apply to state devices, which was done on a continuous cycle. He discussed additional benefits of the cloud migration.

9:56:53 AM

Mr. Smith continued to address slide 7. He discussed the goal of reducing the amount of time a system was vulnerable. He referenced the cost survey he showed earlier. He cited a study that showed that mature cloud modernization reduced the time an organization took to

identify and contain a breach by 77 days. He emphasized the criticality of the speed of reaction.

Senator Wilson asked about a shift in workforce due to the Covid-19 pandemic, and how cyber security would change with an at-home workforce.

Mr. Smith relayed that an at-home workforce was helpful on multiple fronts. He described the advantage of users connecting directly to the cloud environment without using a Virtual Private Network. He explained that the data was present in the cloud in a controlled and secure manner, which meant the state was not beholden to specific fiber pipelines. He thought the resilience in emergent situations had an operational benefit. He summarized that an at-home workforce allowed the state to disengage from some of the more cumbersome and costly data center and network structures currently in place.

10:00:18 AM

Mr. Smith spoke to slide 8, "Technology - Cloud Migration":

Capital Supplemental Request -$23,116.0(HB284/SB165)

Project scope
Assess and migrate ~3000 executive branch servers located throughout the state.

- Discovery, development of SOW/timeline, migration services
- Phased large-scale lift-and-shift approach to achieve significant cloud benefit in shortest amount of time
- Complex modernizations deferred until after migration
- Disaster Recovery, Cloud Storage and Operational costs
- Network costs specific to cloud operations

ROI Implications

- Experience to date: 93 servers in SOA Azure, with an average cost per server of $1,812/year (25% less than current chargeback rates to departments).
- Industry trends indicate total cost of ownership ROI in 4 to 5 years with an average 21% savings (Gartner, 2021)

- Complexity (1,800+ applications across 60+ locations) and cloud-based options adds significant variability

On Premise alternative

~$39 M over 5 years+ Migration Services

- Consolidate remaining servers (~50%) into primary datacenters
- Update aged infrastructure (expand primary datacenters)
- Procure security systems similar to those offered in cloud environment
- Does not provide all cloud-based security benefits (DDoS, shared responsibility, etc.)

10:03:31 AM

Senator Wielechowski asked if the state had made any major technology or IT investments in the previous five years that were now obsolete because of the rising risk of cyber-attacks.

Mr. Smith detailed that the last major refresh of the state's network was over five years previously. The data centers had been kept up to date. He cited that there were a number of servers that had "technical debt," and the replacement models for the servers were part of capital requests. There was a significant number of data servers in the state that were being tracked as vulnerabilities and being mitigated for threat reduction.

Senator Wielechowski asked if the committee should expect any significant capital requests in the following years to deal with the cyber-attacks.

Mr. Smith stated that moving the bulk of the data, applications, and servers to the cloud environment would create more an operational model without significant swings in capital requirements for a lot of equipment. He cited that there could be potential costs for software and security programs, but he did not anticipate significant capital expenditure for the cloud migration.

Co-Chair Bishop asked if the cloud storage repository was inside or outside of Alaska.

Mr. Smith stated that the repository was outside Alaska,

and the Azure environment the state was using for the large-scale migration was a Microsoft public cloud product that resided in data centers all over the world but with none in the state. He added that there was a higher level of security for the state's most secure items, which would be down in the Southwest of the United States.

Senator Wilson asked about the estimated time for a cloud migration of the state and ordering of the departments.

Mr. Smith relayed that the project would use tools that would allow for moving large groups of servers simultaneously. The migration would be a two-phase project. He stated that the first phase would be the Juneau and Anchorage data centers, and the second phase would involve the remaining servers around the state. Each phase would involve cross sections of the departments. The division did not have a firm timeline and expected the project would take 18 to 24 months from start to finish.

10:07:53 AM

Senator Wielechowski asked about Microsoft's security record, since the state would be transferring its data using the companies' technology.

Mr. Smith cited that the security record for Azure was very good and was better than most premise-based systems. He continued that all the public cloud environments were designed with zero-trust type of capabilities to ensure the security of the systems. He clarified that the cloud had structural aspects that made it more secure, with data distributed across via algorithm across multiple servers in different locations. The cloud was also fully encrypted at rest as well as in transit. He noted there was still a role for the state in the security of the data, which his group took very seriously.

Senator Wilson thought Azure had a major flaw in 2019, and Microsoft had uploaded a new feature which left about 3,300 individuals vulnerable to attack. He asked if the state networks were vulnerable to the flaw.

Mr. Smith was not certain he was aware of what Senator Wilson was referencing, nor if the state's servers were involved. He stated that typically large-scale vulnerabilities would affect multiple environments.

Mr. Smith showed slide 9, "Technology – Enterprise Systems":

Cyber security benefits of enterprise systems:

- Microsoft Licensing
  - Multi-factor Authentication & Conditional Access
  - Endpoint/Mobile Device Management and patching
  - Defender Suite (desktop, email, identity)
  - Identity management
- Managed Security Operations integration
  - Common system avoids one off solutions
  - Fully integrated suite of products informed by worldwide intelligence
  - Creates capacity within SOA security professionals

Infrastructure Bill Requests:
- Security tool implementation -$1,149.0
- Managed Security Operation Center-$1,700.0

Mr. Smith pointed out that many programs had an inherent cyber security nexus despite not being solely for cyber security.

10:12:30 AM

Mr. Smith addressed slide 10, "Processes – IT Consolidation":

Single, focused approach to cyber security
- Execute basic protocols well
  - Practice good cyber hygiene
  - Ensure Compliance
  - Enhance response capabilities
  - Immediate threat hunting against security threats
- Simplify the enterprise security environment
  - Speed and efficiency of incident response
  - Integrated systems avoid gaps in coverage
- Continue the path to Zero Trust
  - Assume breach
  - Verify explicitly
  - Least privileged access

Mr. Smith addressed the infographic on the right, which listed things the division was doing, including vulnerability screening, security patching, intelligence sharing, penetration testing, cyber training, incident response, compliance auditing, and threat hunting. He contended that OIT needed more resources to do things better. He discussed cited that about 90 percent of cyber threats could be countered with basic protocols.

Mr. Smith continued to address slide 10. He commented on the complexity of the state's environment. He noted that there was a correlation between complexity and incident cost, and many of the state's efforts were aimed at simplifying the landscape. He discussed the zero-trust path and mentioned multi-factor authentication.

Mr. Smith summarized that there was an extremely high threat environment that was not diminishing, and there were highly qualified and dedicated IT professionals within the state workforce that were protecting the state very well given the challenges. The division worked to have zero breaches, and the team had been working hard towards the goal. He commented that the team could not maintain the status quo, and OIT was looking to improve in three areas: people and training, technology with the cloud and other systems, and consolidation.

Co-Chair Stedman relayed that any member could request a private meeting to get more detail on the questions that had been discussed. He mentioned the possibility of the committee going into executive session. He wanted to start with individual meetings to avoid the necessity of an executive session.

Co-Chair Stedman thanked Mr. Smith for his testimony.

Co-Chair Stedman discussed the agenda for the afternoon, at which time the committee would consider a Committee Substitute for SB 164, which he thought could be the final capital budget bill.

#
ADJOURNMENT
10:17:52 AM

The meeting was adjourned at 10:17 a.m.