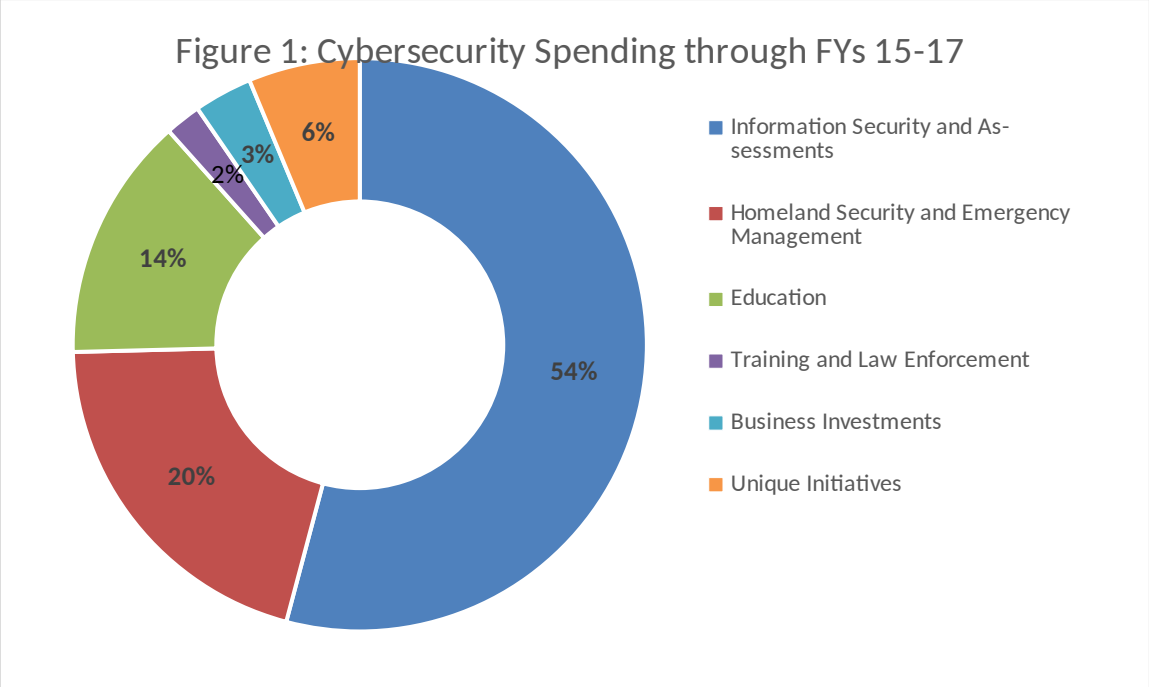
States Confront the Cyber Challenge
Memo on State Cybersecurity Budgets

General Overview

Funding and sustaining cybersecurity initiatives is one of the fundamental challenges confronting state policy makers. A recent survey of states found that, on average, cybersecurity funding only accounted for three to five percent of information technology (IT) budgets.[1] This memo examines how 23 states and the District of Columbia (D.C.) have allocated resources for cybersecurity and how they measure their return on investment. Throughout Fiscal Years (FY) 2015, 2016, and 2017, these 24 states spent over $160 million on six categories of cybersecurity: (1) Information Security and Assessments; (2) Homeland Security and Emergency Management; (3) Education;[2] (4) Training and Law Enforcement; (5) Business Investments; and (6) Unique Initiatives. Figure 1 highlights how the states allocated funds in these categories. The tables at the end of the memo break out each state's appropriation by category.



Methodology

All 50 states' and the District of Columbia's enacted budgets from FYs 2015-2017 were examined for this memo. To identify cybersecurity expenditures in the budgets, "information

[1] National Association of Chief Information Officers. (2016). *2016 Deloitte-NASCIO Cybersecurity Study.* Retrieved from http://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

[2] Florida devoted $14.5 million in FY16 to industry certifications that included several sectors, including cybersecurity.

security," "technology security," and "cybersecurity/cyber security" were key words used to filter information. Only line-item expenditures are included in this memo. Therefore, cybersecurity spending may have been incidentally omitted if it was part of a larger budget allocation. Additionally, a macro trend analysis was not conducted due to only three years of collected data; yet, when possible, budget trends were mentioned within and across states. Due to these limitations, this memo is not intended to holistically capture all state cybersecurity spending. Rather, it provides insight into how some states are allocating their budgets to cybersecurity and highlights unique state-funded initiatives across the nation.

Information Security and Assessments

Information security and assessments was the largest funded area with roughly $85 million devoted to these initiatives across 15 states. This category comprises any broad funding appropriated to IT security offices, IT security enhancements, asset monitoring, data protection, and other broad investments geared toward defending the state's IT backbone. States combined expenditures in this category were $30 million in FY15, rose to $34 million in FY16, and dropped to $22 million in FY17. In FY15 alone, **South Carolina**'**s** spending accounted for half of all the states' expenditures. In FY16, notable spending included $5-8 million in **Michigan, Missouri,** and **Texas** for cybersecurity improvements and protection of information. In FY17, **Virginia**, spent over $4.3 million for an IT security service center to help state agencies protect their networks. Yet, **Idaho** and **Florida** showed that states do not necessarily need to spend millions of dollars to enhance cybersecurity in the state. **Idaho** devoted $141,000 to implement a cybersecurity process that only allows users to access resources that are needed to perform a job, thereby decreasing user access to sensitive assets. In **Florida**, roughly $250,000 is being spent per agency to complete an information risk assessment. Although the total cost of this program is contingent upon the number of agencies assessed, it nonetheless illustrates a relatively low cost option that can be gradually rolled out. Through these risk assessment, agencies can identify and assess security risks; identify risks' severity; recommend remediation strategies; prioritize remediation activities; estimate the schedule and cost for the remediation plan; and work with the state's IT agency to develop an implementation plan.

Homeland Security and Emergency Management

Homeland security and emergency management funding was the second highest expenditure area at over $32 million across seven states.[3] Activities funded under this category include overall homeland security initiatives and cybersecurity terrorism/defense task forces/units. **Michigan** leads states in this area, spending $9 million and $13 million for cybersecurity in homeland security in FY15 and FY16, respectively. Fusion centers also saw increased funding as **Georgia** appropriated roughly $200,000 to add two analysts to work in the fusion center to assist with cyber terrorism intelligence. In **Washington**, emergency communications received over $2.6 million for cybersecurity measures to protect their emergency services IP network, which supports 9-1-1 call centers.

Education

University systems play two critical functions within the states' cybersecurity ecosystem. First, they hold a wealth of personal identifiable information and host valuable intellectual property—both of which are attractive targets for adversaries. Secondly, they are key to improving a state's cybersecurity by grooming the future cadre of state cybersecurity employees. As a result, **Colorado** has invested about $1 million for asset management and disaster recovery for

[3] Louisiana's appropriations were not included in the total expenditures because there was not a line item budget to the total $1.3 billion. Part of that fund was used to "deploy proprietary cyber security information database tool to identify private sector Critical Infrastructure/Key Resources (CI/KR) networks that are exposed to malicious cyber threats."

education systems from FY16-FY17. In **Idaho**, $1 million was appropriated to build a cybersecurity lab that allows university students to use their cybersecurity skills on software, hardware, and engineering systems. Similarly, **Virginia** recently appropriated $4 million to create a cyber range that allows students to test their cybersecurity knowledge in a secure network. Additionally, **Virginia**, along with **Florida**, provided funds for cybersecurity certifications, scholarships for service, and to assist colleges become certified by the National Security Agency as Centers of Academic Excellence.

Training and Law Enforcement

Equally important to educating future cybersecurity personnel is training current staff. **Florida** set aside over a half million dollars for information security training for information security managers and their staff who use the state's data center. Additionally, **Florida** devoted over $50,000 for information security training for several state agencies and provided a line-item of about $300,000 for cybersecurity training to their department of law enforcement. **Maine** also contributed funding to their department of public safety for computer crimes training. Although **Florida** and **Maine** were the only states that explicitly set aside this type of funding for law enforcement, it may become a growing trend in the future as law enforcement gains a larger role in states' cybersecurity ecosystems. This was evident in **Michigan**, which devoted over $2 million to the state police to expand efforts to combat cyber crimes.

Business Investments

Discussions surrounding cybersecurity often focus on the threat of damaging breaches. However, the other—and brighter—side of cybersecurity is the beneficial economic impact it can have in a state. **Maryland** and **Virginia** are two leaders who recognize the economic value that cybersecurity presents. Since FY15, **Maryland** has contributed $4.7 million to "stimulate and attract private investments in early-stage cybersecurity technology businesses."[4] Specifically, the state has two programs that provide seed money and an income tax credit to help businesses become more attractive for acquisition or equity investment. **Virginia** takes a different approach through a business accelerator called Mach37, which was given $500,000 in FY17. Through Mach37, cybersecurity entrepreneurs engage with mentors over 90 days to launch their own cybersecurity start up. Both programs act as vehicles to continuously provide new jobs to cybersecurity graduates and therefore increase the state's tax base.

Unique Programs

Outside of these large categories, states are meeting the cyber threat by funding unique state initiatives. Most recently, **Colorado** launched an $8 million cyber program to create the National Cybersecurity Center. The Center will serve three purposes: (1) to help businesses, nonprofits, and government agencies combat, respond, and recover from cyber attacks; (2) to educate government officials about cybersecurity; and (3) to provide research and development in future cybersecurity technology.[5] In **Florida**, the state is actively assisting their local partners by allocating funds to help a county launch a cybersecurity defense initiative. Lastly, **Virginia** detailed $800,000 to assist military veterans obtain cybersecurity jobs.

Return on Investment

Determining the effectiveness of a cybersecurity program can be difficult to assess. For example, it may not be possible to prove whether a certain program or policy prevented a malicious intrusion. However, seven states, through their budgets, explicitly detail how they measure their return on investment (ROI). **Connecticut**, **D.C.**, **New Jersey**, and **Washington** assess how many

[4] http://dbm.maryland.gov/budget/FY2016FiscalDigest/complete.pdf
[5] http://www.statebillinfo.com/bills/bills/16/1453_enr.pdf

cyber attacks were blocked (such as phishing emails, denial of services attacks, and unauthorized access), percent of downtime due to cybersecurity attacks, percent of critical vulnerabilities remediated in 60 days, and number of security incidents caused by non-compliance. Unlike **Connecticut**, **D.C**., and **Washington**, **New Jersey** details additional ways of assessing ROI by leveraging their cybersecurity and communications integration cell (NJCCIC). These evaluation indicators include assessing cyber analyses through the amounts of threat and situational reports published by the NJCCIC; measuring the level of pubic private partnerships through the amount of new members registered with the NJCCIC; and evaluating cybersecurity awareness via briefings and webinars.

Maryland, **Texas**, and **Washington** take a different approach to measure their ROI. **Maryland** and **Texas** measure the percent of executive branch employees compliant with statewide cybersecurity awareness training programs; number of state agency security assessments performed; and the number of state agencies that participate in provided security training offerings. In **Washington**, an agency must answer several questions before it can receive funding. These questions include: What are the consequences of adopting or not adopting this package? What alternatives were explored by the agency and why was this package chosen? What are the other important connections or impacts related to this proposal? Although these questions are not cybersecurity specific, it allows for state IT professionals to translate the need for cybersecurity proposals to state legislators.

Lastly, **Virginia** is unique because they attach an ROI to their cybersecurity business accelerator, Mach37. Mach37's is evaluated based on the number of companies assisted and the number of startups successfully launched through the accelerator; the number of companies operating in Virginia as a result of the program; estimated number of jobs created; the value of proceeds from the sale of equity in companies that received capital support from the program; the number of state investments that failed and the state investment associated with failed investments; and the number of new companies created or expanded and the number of patents filed.

Looking Ahead

Since not all state budgets offer line item details, it is difficult to ascertain true gaps in cybersecurity funding. However, based on the information identified in developing this memo, three gaps emerge: protecting public hospitals, investing in K-12 education, and investing in the cybersecurity economy. Both public and private hospitals are becoming growing targets, which could have potential economic and physical consequences for hospital patients. And although states are investing in their university systems, there is still a need to invest in computer science curriculums in K-12 classes by ensuring teachers have the necessary skills and tools to adequately teach computer science courses. Lastly, there is a growing need to invest in business opportunities and to adopt programs such as those in **Maryland** and **Virginia**, which can provide economic opportunities for the state.

As states invest in "core cyber capabilities"—hardening their networks, supporting their IT security offices, and contributing funds to homeland security and emergency management offices —they must strategically think about emerging challenges, such as the workforce development gap, so that they may adequately protect their citizens from cyber threats.

Please e-mail Michael Garcia, Policy Analyst, Homeland Security and Public Safety Division, NGA at: mgarcia@nga.org *with any questions.*

Table 1-Information Security and Assessments Spending

State	Program		Total Funding
CA	Information Security Office FY16		$1,600,000
CO	Risk Management Information System FY16		$137,488
DC	Information Security Office FY15		$4,973,000
DE	Security Office	FY15 $1,300,000	$2,545,000
		FY16 $1,245,000	
FL	Risk assessments for each state agency FY16		$254,167
ID	"Least Privilege" software	FY16: $141,000	$6,508,700
	Data Loss Prevention Software	FY16: $250,000	
	Defend against cyber attacks	FY16: $6,117,700	
ME	Creates two new positions to enhance cybersecurity	FY16: $212,268	$428,006
		FY17: $215,738	
MI	Cybersecurity IT Investment projects	FY15: $2,000,000	$9,000,000
		FY16: $2,000,000	
	Cybersecurity Improvements	FY16: $5,000,000	
MO	IT Security Enhancements	FY15: $6,000,000	$16,000,000
		FY17: $2,000,000	
	Cybersecurity Enhancements	FY16: $8,000,000	
NC	Enterprise Security and Risk Management	FY17: $400,000	$957,285
	IT Security Equipment	FY17: $557,285	
NJ	Cybersecurity and Data Protection	FY16: $3,000,000	$7,000,000
	Cyber	FY17: $4,000,000	
OR	Information Security Management Program FY15-17		$922,171
SC	Total Division of Information Security FY15		$15,235,993
TX	Enhance cybersecurity efforts	FY16: $5,774,504	$12,449,008
		FY17: $5,774,504	
	Cybersecurity advancement for Aging and Disability, and Family and Protective Services	FY16: $900,000	
VA	Computer Operations Security Services	FY17: $3,260,657	$7,608,986
	IT security service center	FY17: $4,348,329	
TOAL FUNDING			**$85,619,804**

Table 2-Homeland Security and Emergency Management

State	Program		Total Funding
CA	Cyber Network Defense Team FY16		$582,000
GA	Cybersecurity Program in Emergency Mgmt. Agency	FY16: $250,000	$259,122
	Two analysts to work on cyber terrorism intelligence in Fusion Center	FY17: $209,122	
LA	deploy proprietary cyber security information database tool to identify private sector Critical Infrastructure/Key Resources (CI/KR) networks that are exposed to malicious cyber threat FY16		Part of $1,278,943,147
MI	Homeland security initiative/cyber security	FY15: $9,063,500	$22,181,700
		FY16: $13,118,200	
NJ	Homeland Security, Cyber FY17		$6,193,000
RI	Cyber Terrorism Task Force	FY15: $100,000	$508,000
	Homeland Security Cyber Unit	FY16: $408,000	
WA	Cybersecurity Measures (Firewalls) for ESInet FY16		$2,662,828
TOAL FUNDING			**$32,386,650**

Table 3-Education

State	Program		Total Funding
CO	Cyber Disaster Recovery for Education	FY16: $19,722	$901,590
		FY17: $19,722	
	Asset Management	FY17: $862,146	
FL	District workforce education programs for students who earn cybersecurity certifications	FY16: $4,500,000	$14,500,000 (Only a portion goes towards cyber)
	Cybersecurity certifications for college students	FY16: $10,000,000	
ID	Cybersecurity Lab FY16		$1,000,000
VA	Cyber Range	FY17: $4,000,000	$5,432,000
	Scholarship for Service	FY17: $1,000,000	
	Centers of Academic Excellence	FY17: $432,000	
TOTAL FUNDING			**$21,833,590**

Table 4-Training and Law Enforcement

State	Program		Total Funding
FL	Information security training for information security managers and staff	FY16: $527,981	$869,759
	Cybersecurity training for Dept. of Law Enforcement	FY16: $291,490	
	Information Security training for several agencies	FY16: $50,288	
ME	Computer Crimes Training	FY16: $85,769	$135,965
	Tech costs for computer crimes division	FY16: $25,048	

	Tech costs for computer crimes division	FY17: $25,148	
MI	Expanding efforts to combat cyber crimes in state police FY16		$2,203,200
TOTAL FUNDING			**$3,208,924**

Table 5-Business Investments

State	Program		Total Funding
MD	Cybersecurity investment fund	FY15: $800,000	$4,700,000
		FY17: $900,000	
	Cyber Investment Incentive Tax Credit Program	FY16: $1,000,000	
		FY17: $2,000,000	
VA	Mach37 FY17		$500,000
TOTAL FUNDING			**$5,200,000**

Table 6-Unique Initiatives

State	Program		Total Funding
CO	Cyber Program FY17		$8,000,000
FL	Orange County Cybersecurity Defense Initiative	FY16: $182,000	$632,000
	National Cyber Partnership	FY16: $450,000	
RI	Cybersecurity Officer FY16		NA
VA	Cybersecurity Commission	FY17: $500,000	$1,300,000
	Assisting Military Veterans obtain cybersecurity careers	FY17: $800,000	
TOTAL FUNDING			**$9,932,000**