



## Building a Successful Cybersecurity Program

Impact Day, 06/07/2019

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

# The next hour...

## **Cybersecurity Program – Organize to succeed**

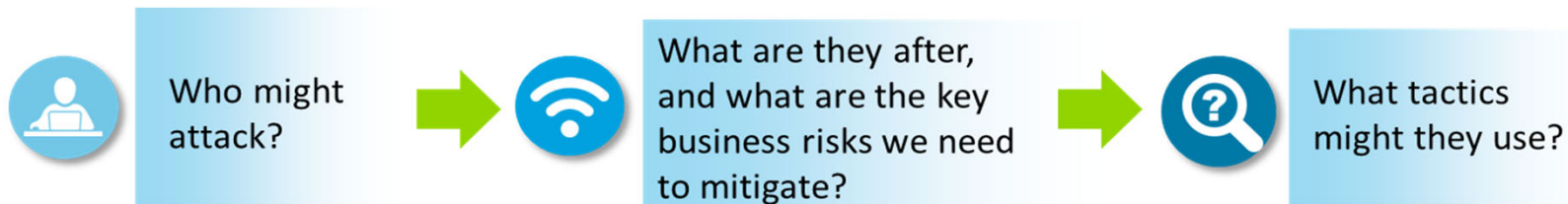
1. Identify Cyber Risks
2. Develop a Cybersecurity Strategy and Plan
3. Align to Business
4. Build a Roadmap and Obtain Funding
5. Communicate Progress

# **1. Identify cyber risks**

## Understand your organization and identify cyber risks

1. What are the assets in the organization?
2. Of those assets, which ones contain sensitive information?
3. If the sensitive information is subject to loss or breach, what are the financial and reputational risks?
4. What are the threats and vulnerabilities that provide the greatest exposure to your organization?
5. To what extent do we have capabilities and practices in place to protect critical assets?
6. How effective are we at monitoring and detecting cyber incidents?
7. Can we effectively respond to and recover from a cyber incident? Do we have response plans in place, and have they been tested?
8. What metrics demonstrate that we are effectively protecting the organization?
9. Is cybersecurity an executive leader priority item?

## Need to Understand threats and motives relevant to your environment

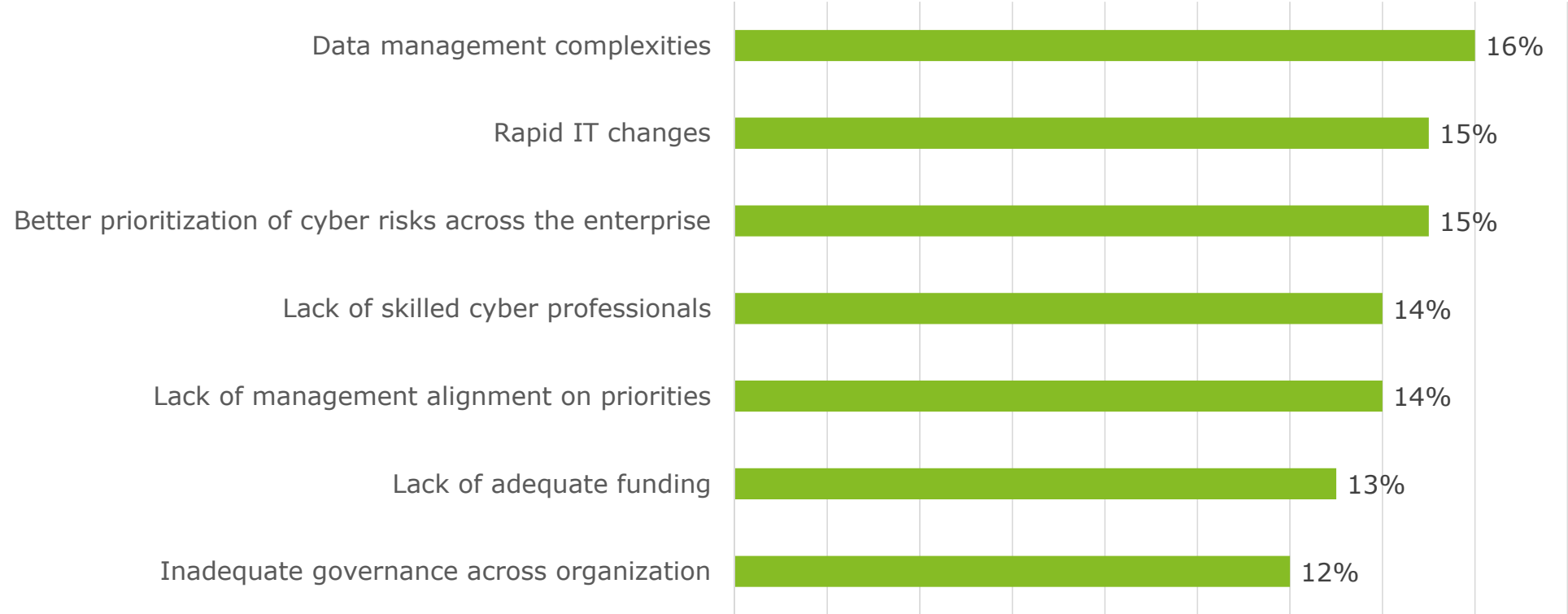


IMPACTS \ ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life safety	Regulatory
Organized criminals	Very high	Moderate	Moderate	Moderate	High	Moderate	Moderate
Hactivists	Moderate	Moderate	Very high	Moderate	Very high	Moderate	Moderate
Nation states	Moderate	Moderate	Very high	Moderate	Moderate	Moderate	Moderate
Insiders / Partners	Very high	Moderate	High	Moderate	High	Moderate	Moderate
Skilled individual hackers	Moderate	Moderate	High	Moderate	High	Moderate	Moderate

KEY    Very high    High    Moderate    Low

# Challenging Aspects of Cyber security management

Participants were asked to select their cybersecurity management challenges



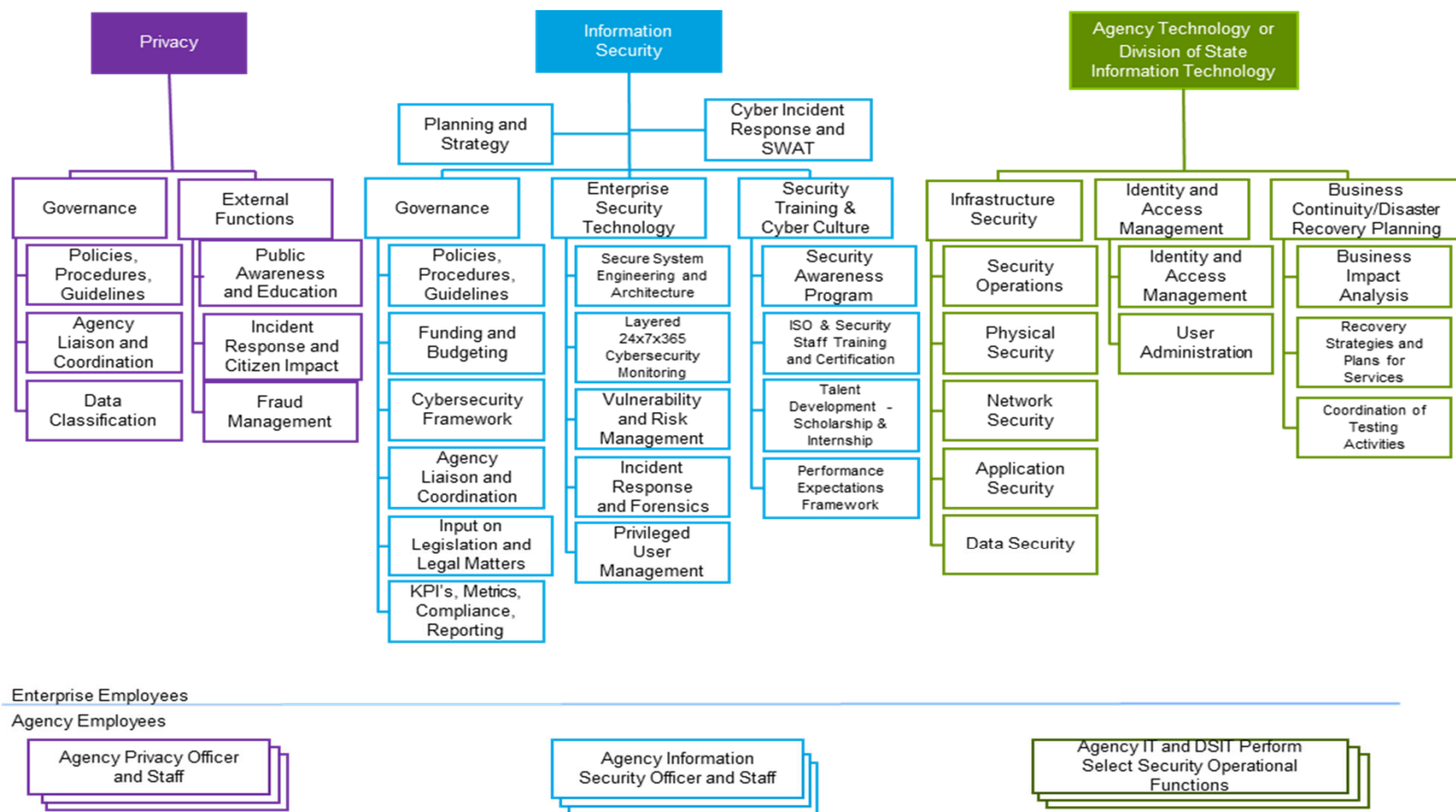
## **2. Develop a Cybersecurity Strategy and Plan**

## Sample Cybersecurity Program Considerations





# Overview of the Technology and Security Operations, Information Security and Privacy Functions – Example State Gov Org mode



# **3. Align to Business**

## Ask the right questions

### First and foremost: understand your business

- Agenda, mission and priorities of the agency head

### Understand cyber risks to the business agenda

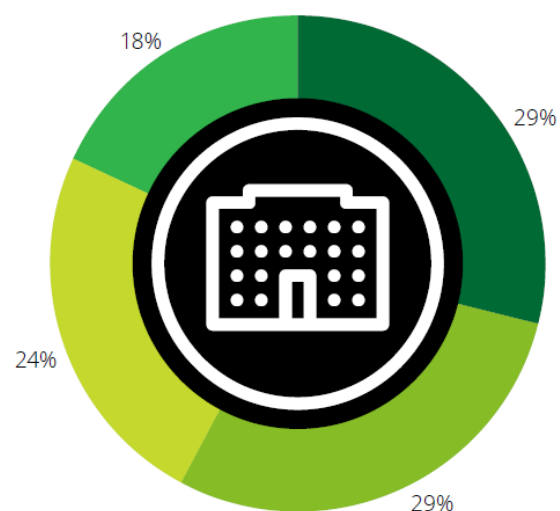
- Where are my high-risk assets?
- Where does the data reside?
- What are the citizen privacy issues?
- Why does the citizen data need to be protected?
- What are the possible motives of an attack based?
- What is the business implication of a breach within the agency, state and external parties?
- What systems are in place to manage risks and where are they?



The future of cyber demands alignment and collaboration both internally and outside the organization



### Cyber department's interaction with other business units



- Through security assessments or audits
- Through security steering committees that work with businesses
- Through separate security organizations within each business
- Through security liaisons/champions within each business

Deloitte The future of cyber survey 2019

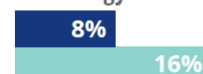
Copyright © 2019 Deloitte Development LLC. All rights reserved.

### Both business stakeholders and technology decision-makers are more actively engaged in defining their state cybersecurity strategy

Line-of-business decision-makers only



Technology decision-makers only



Both line-of-business and technology decision-makers



Neither line-of-business nor technology decision-makers



Not applicable/do not know



2018 2016

2018 Deloitte-NASCIO Cybersecurity Study

#StateofCyber

Impact Day 2019

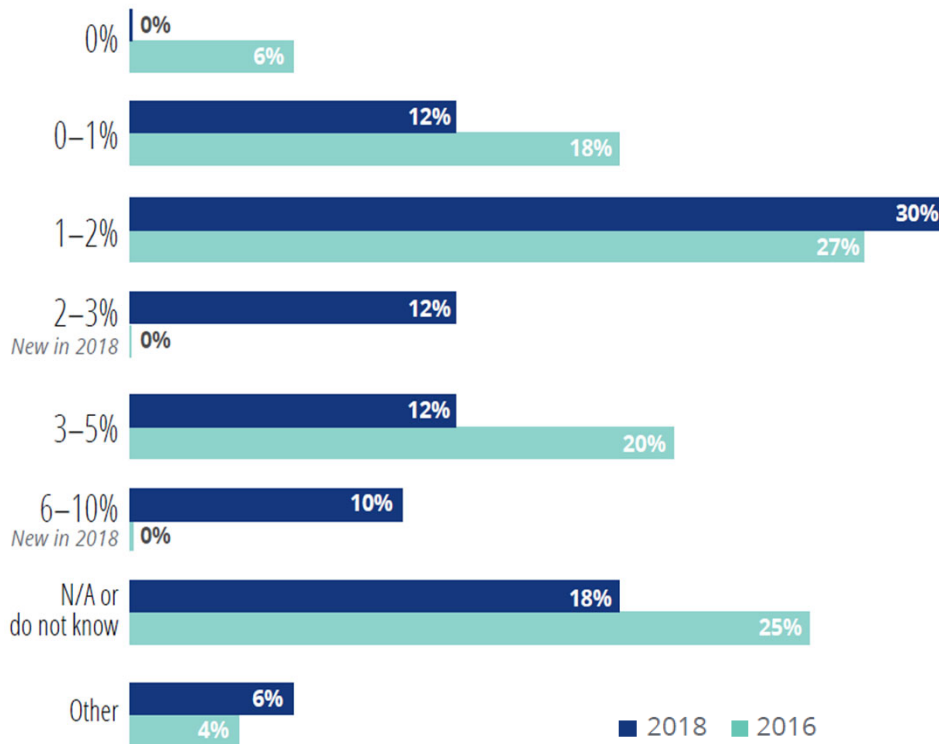
# **4. Build a Roadmap and Obtain Budget**

## An example: Progress of the State Government

	Build foundation	Evolve	Leading in class
People	Establish Organization	Develop performance expectation framework	Develop statewide metrics and monitoring
	Establish COO, CISO, CPO	Identify talent strategies	Grow and retain talent
	Establish Deputy CISOs, Deputy CPOs	Conduct joint performance reviews	Implement broad professional development
	Establish awareness and training	Develop cybersecurity programs with universities	Effective and collaborative governance
	Professional development program		Mature cybersecurity talent sourcing program with local universities
IT Security Process	Define security framework	Mature security policies, procedures, and standards	Automate security functions (access management, monitoring, etc.)
	Establish data classification framework	Gather agency security plans	
	Define security policy	Establish ongoing compliance program	
	Conduct security risk assessments and define risk profiles for agencies	Mature incident response team	
	Apply data protection policy		
IT Security Technology	Conducted continuous vulnerability assessment	Continuous threat and vulnerability management	Develop secure self-healing infrastructure
	Discover statewide data	Develop agency security shared services	Implement governance, risk, and compliance tools
	Implement data protection technology	Implement data loss prevention	Develop agency centers of excellence
	Implement threat monitoring and control	Implement identity and access management	
	Implement secure network engineering	Develop cyber threat analytics and intelligence	
			<div>Not Started</div> <div>In Progress</div> <div>Completed</div>

Budget continues to be a challenge

## Most states only spend 0-3% of their IT budget on cybersecurity



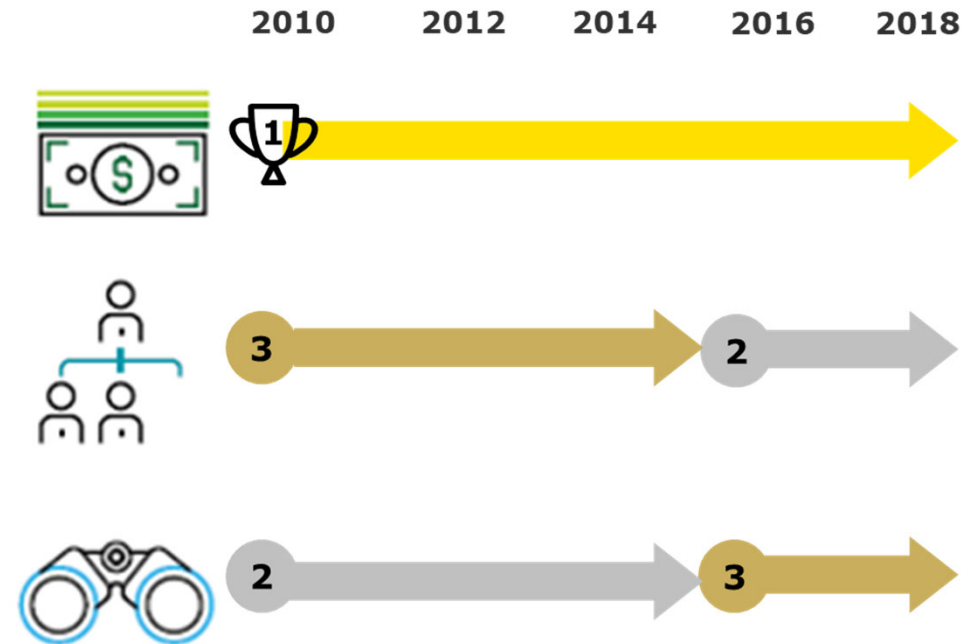
2018 Deloitte-NASCIO Cybersecurity Study

Copyright © 2019 Deloitte Development LLC. All rights reserved.



**Deloitte.**

## Budget, talent, and threats rank the top three since 2010



#StateofCyber

Impact Day 2019

# **5. Communicate Progress**



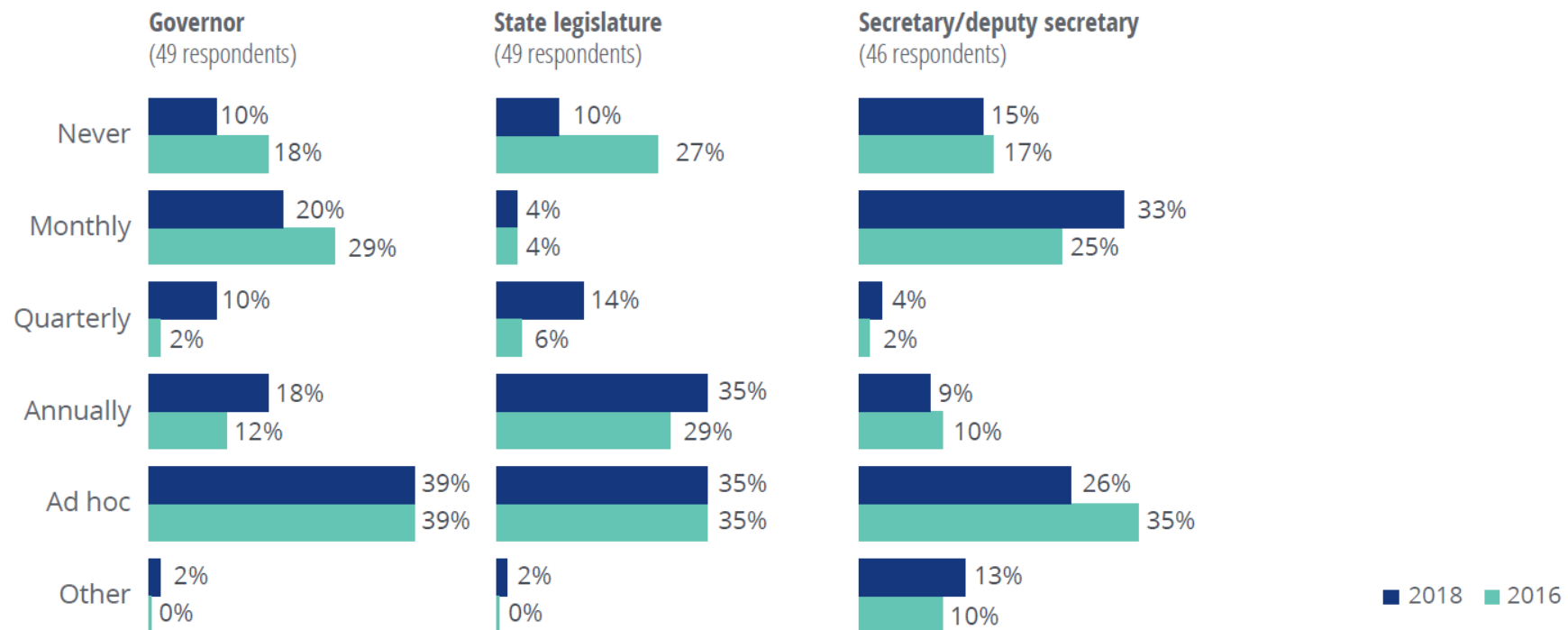
## Moving forward... Strategize & achieve appropriate funding

- Communicate and collaborate with legislators and state business/program leadership to build a business case for security as a line item in the budget
- Effectively collaborate with agency-level program and business leaders to get cybersecurity included in program budgets
- Work with CIOs to:
  - Allocate a reasonable percentage of new business and technology initiatives for cybersecurity
  - Identify creative ways to include cybersecurity as a critical part of enterprise data center consolidation initiatives

## Governor-level cyber awareness is on the rise



To what extent are you required to provide reports on cybersecurity status or posture of the enterprise?



The 2018 Deloitte-NASCIO Cybersecurity Study

Copyright © 2019 Deloitte Development LLC. All rights reserved.

#StateofCyber

Impact Day 2019

# Bold Plays for Change

2018 Deloitte-NASCIO Cybersecurity Study



## ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

CISOs should raise cybersecurity's visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies' security mandates.



## CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER



CISOs should actively participate in shaping the state's innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.



## TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

CISOs should leverage public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private-sector firms.



**Deloitte.**



#StateofCyber

## About the presenters

### **Mike Wyatt**

Principal, State Sector Risk Advisory Leader  
Deloitte & Touche LLP

### **Bharane Balaubramanian**

Sr. Manager, State Sector Risk Advisory  
Deloitte & Touche LLP

### References:

#### **The New CISO - Leading the strategic security organization**

Deloitte Review Article 19, Taryn Aguas, Khalid Kark, and Monique François, July 2016

<https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html>

#### **The Future of Cyber Survey 2019**

<https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html>

#### **2018 Deloitte-NASCIO Cybersecurity Study: Bold Plays for Change**

<https://www.nascio.org/Publications/ArtMID/485/ArticleID/730/2018-Deloitte-NASCIO-Cybersecurity-Study-States-at-risk-Bold-plays-for-change>



### **About Deloitte**

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte's cyber risk services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation, and performance objectives through proactive management of the associated cyber risks. Deloitte provides advisory, implementation, and managed cybersecurity services to help our government clients lead the way with a collaborative threat intelligence strategy. Deloitte's demonstrated approach and methodology help our clients better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to deliver services in the face of cyber incidents.

The Deloitte Center for Government Insights produces groundbreaking research to help government solve its most complex problems. Through forums and immersive workshops, we engage with public officials on a journey of positive transformation, crystallizing insights to help them understand trends, overcome constraints, and expand the limits of what is possible.

For more information, visit [www.deloitte.com](http://www.deloitte.com) or read about the Deloitte Center for Government Insights at [www.deloitte.com/us/center-for-government-insights](http://www.deloitte.com/us/center-for-government-insights).

### **About NASCIO**

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories, and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research, publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs.

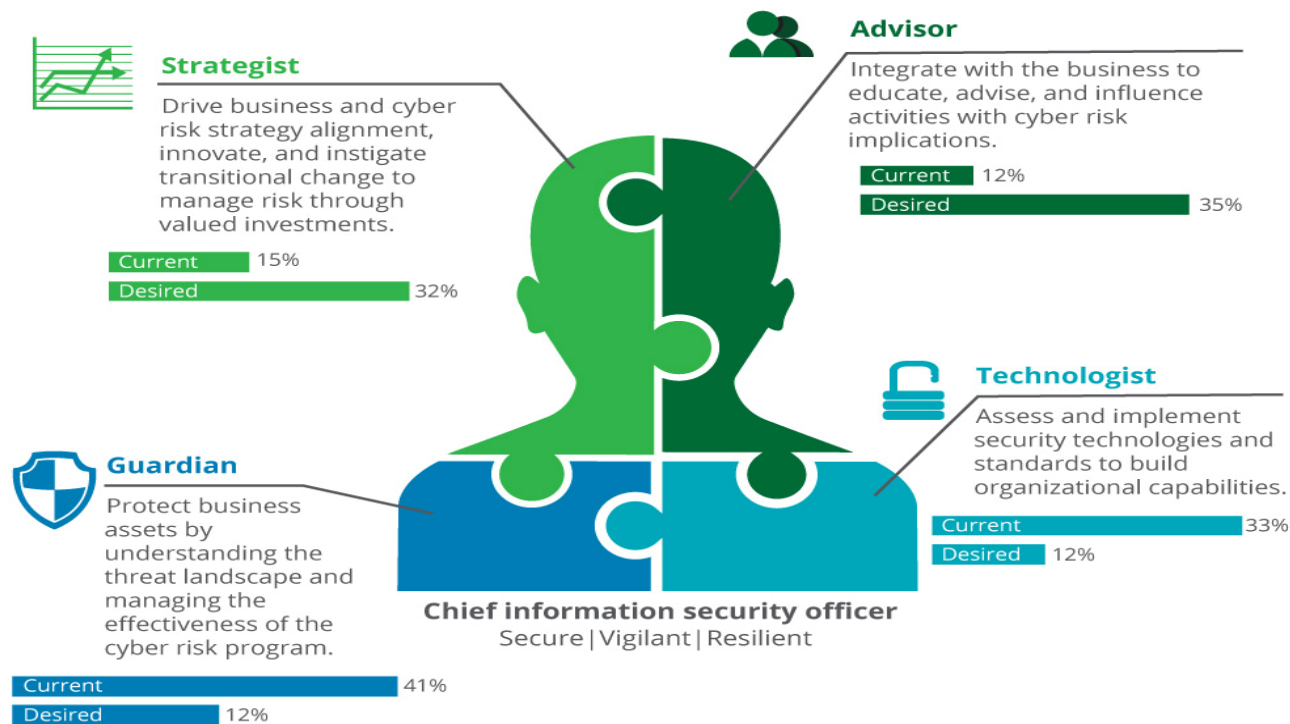
For more information, visit [www.nascio.org](http://www.nascio.org)

# Appendix - Transitioning to a CISO

## Consider where you spend your time

As a new executive, there will be endless demands on your time. The most successful CISOs determine early on how to balance their time and energy across four critical roles

Figure 2. The four faces of the CISO



Source: Research from Deloitte's CISO Transition Labs.

Graphic: Deloitte University Press | DUPress.com