Managing Cyber Risk

The imperative to become Secure, Vigilant and Resilient

Public Sector – State Government

State governments are a target; in addition to financial impact, state cyber issues impacts citizen trust

States collect, share and use large volume of the most Comprehensive Citizen Information

- Data loss from government impacts citizen trust and has the potential to impact state business by affecting citizen services, revenue collections, or unplanned spending.

Makes them an Attractive Target for both Organized Cyber Criminals and Hactivists

Hactivist groups are distinct from more well established cyber criminal organizations in both:

- **organizational structure:** ad-hoc vs. top-down
- and **motivation**: "hacktivism" vs. monetary gain.

Consequently, Cybersecurity is becoming a Governor Level Issue

- Cause: Recent prominent and sophisticated state level cyber attacks impact citizen trust
- Effect: Maryland Governor O'Malley and Michigan Governor Snyder co-sponsor a National Governors Association (NGA) Resource Center on Cybersecurity. The "National Policy Council for State Cybersecurity" is formed to provide recommendations for state governors.

Government uses technology and innovation to improve citizen services and efficiency, which also create cyber risk

- **Threat actors exploit weaknesses that are byproducts of growth and technology innovation.**
  - Rapid modernization of legacy systems
  - Web enablement of citizen services
  - New sourcing and supply chain models
  - New applications and mobility tools
  - Use of new technologies for efficiency gains and cost reduction
  - Increasingly mobile workforce

- **Perfect security is impossible.**
  The goal is to manage risk by becoming:
  - **SECURE —**
    Enabling business innovation by securing critical assets against known and emerging threats across the ecosystem
  - **VIGILANT —**
    Reducing detection time and developing the ability to detect the unknown
  - **RESILIENT —**
    Strengthening your ability to recover when incidents occur

In April 2012, the State of Utah data breach has compromised personal health information of up to 780,000 people[1]

3.5 million records exposed on Texas Comptroller's server[2]

South Carolina Revenue Department server is hacked[3]

Cyber threats are asymmetrical risks

- Small, highly skilled groups exact disproportionate damage
- They often have very targeted motives
- They're spread across the globe, often beyond the reach of law enforcement
- Threat velocity is increasing, response window is shrinking
- Attacks can happen over long periods of time, and in a stealthy manner

Cyber risk strategy must be a component of leadership strategy, and can't simply be delegated to IT.

Sources:

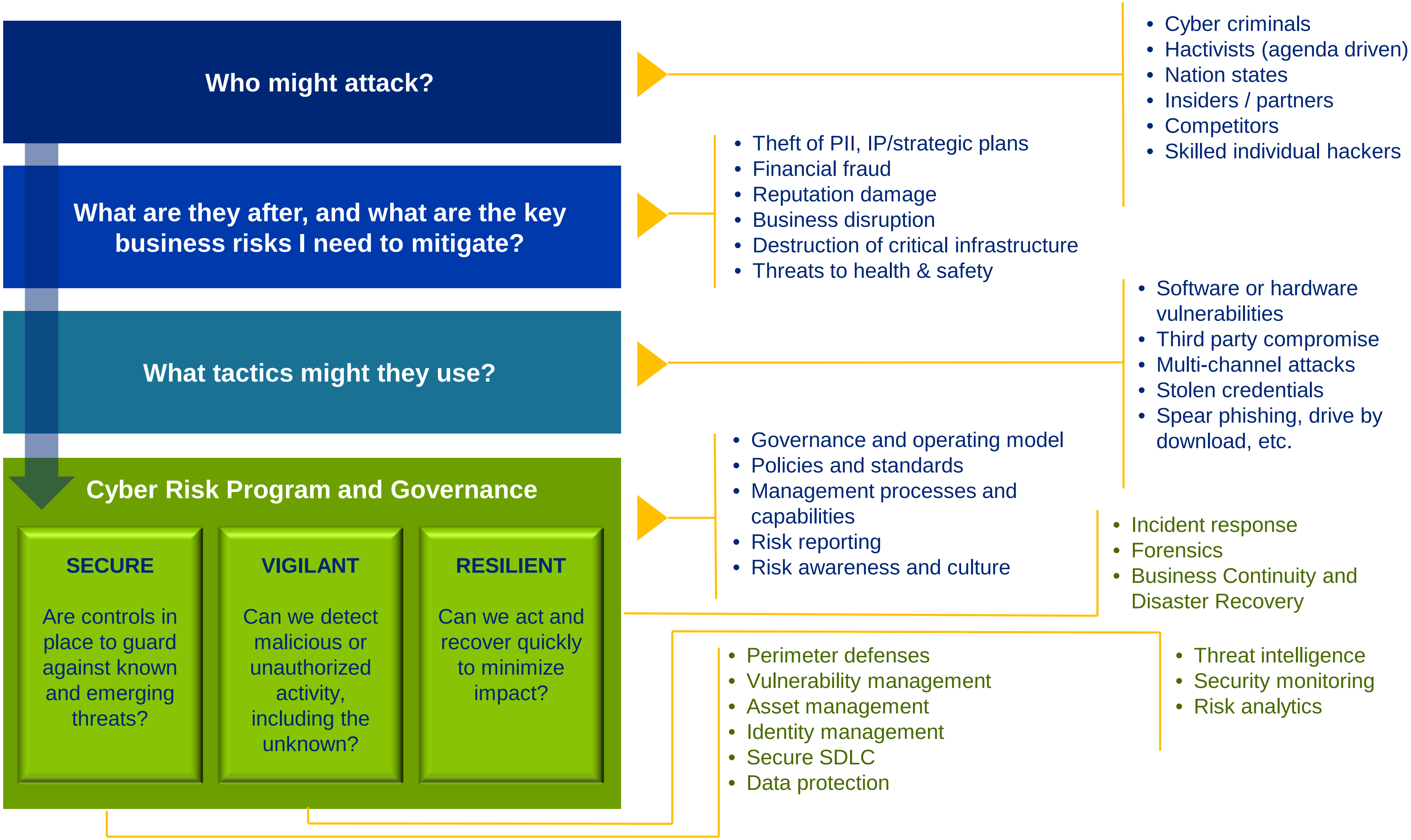
[1] *http://www.health.utah.gov/databreach*

[2] *Security Week, 4/11/2011*

[3] *USA Today, 10/26/2012*

Understanding the threat landscape

It starts by understanding who might attack, why, and how



Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- Nation states
- Insiders / partners
- Competitors
- Skilled individual hackers

What are they after, and what are the key business risks I need to mitigate?

- Theft of PII, IP/strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety

What tactics might they use?

- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials
- Spear phishing, drive by download, etc.

Cyber Risk Program and Governance

- Governance and operating model
- Policies and standards
- Management processes and capabilities
- Risk reporting
- Risk awareness and culture

SECURE

Are controls in place to guard against known and emerging threats?

- Perimeter defenses
- Vulnerability management
- Asset management
- Identity management
- Secure SDLC
- Data protection

VIGILANT

Can we detect malicious or unauthorized activity, including the unknown?

- Threat intelligence
- Security monitoring
- Risk analytics

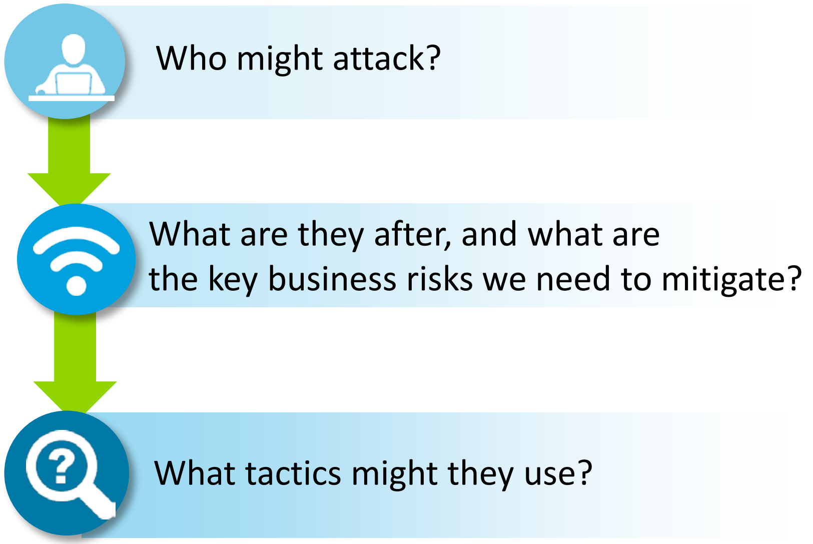
RESILIENT

Can we act and recover quickly to minimize impact?

- Incident response
- Forensics
- Business Continuity and Disaster Recovery

Cybersecurity continues to be one of the most pressing challenges

A typical cyber risk heat map for the State Governments



Who might attack?

What are they after, and what are the key business risks we need to mitigate?

What tactics might they use?

MOTIVES / ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Reputation damage	Business disruption	Destruction of critical infrastructure
Organized criminals	■	□	▩	□	□
Hactivists	□	□	■	■	□
Nation states	□	□	□	■	▨
Competitors					
Insiders / Partners	■	□	▩	▩	□
Skilled individual hackers	▨	□	▩	▩	□

KEY ■ Very high ▩ High ▨ Moderate □ Low

Notable insights from the 2012 Deloitte-NASCIO Cybersecurity Study[1]

- Cybercriminals and hacktivists use increasingly sophisticated methods involving rapidly evolving technologies to target cyber infrastructure for monetary gain and to make political statements.
- Insufficient funding is still the greatest hurdle CISOs face.
- When PII goes public, it can spur some of the most heated citizen outrage and damning media attention.
- The economic costs from breaches are substantial. The annual Ponemon study[2] puts the organizational cost per breach at $5.5 million—a hefty penalty that financially strapped states can little afford.
- Emerging cybercrime and state-sponsored threats will require a strong response from states.

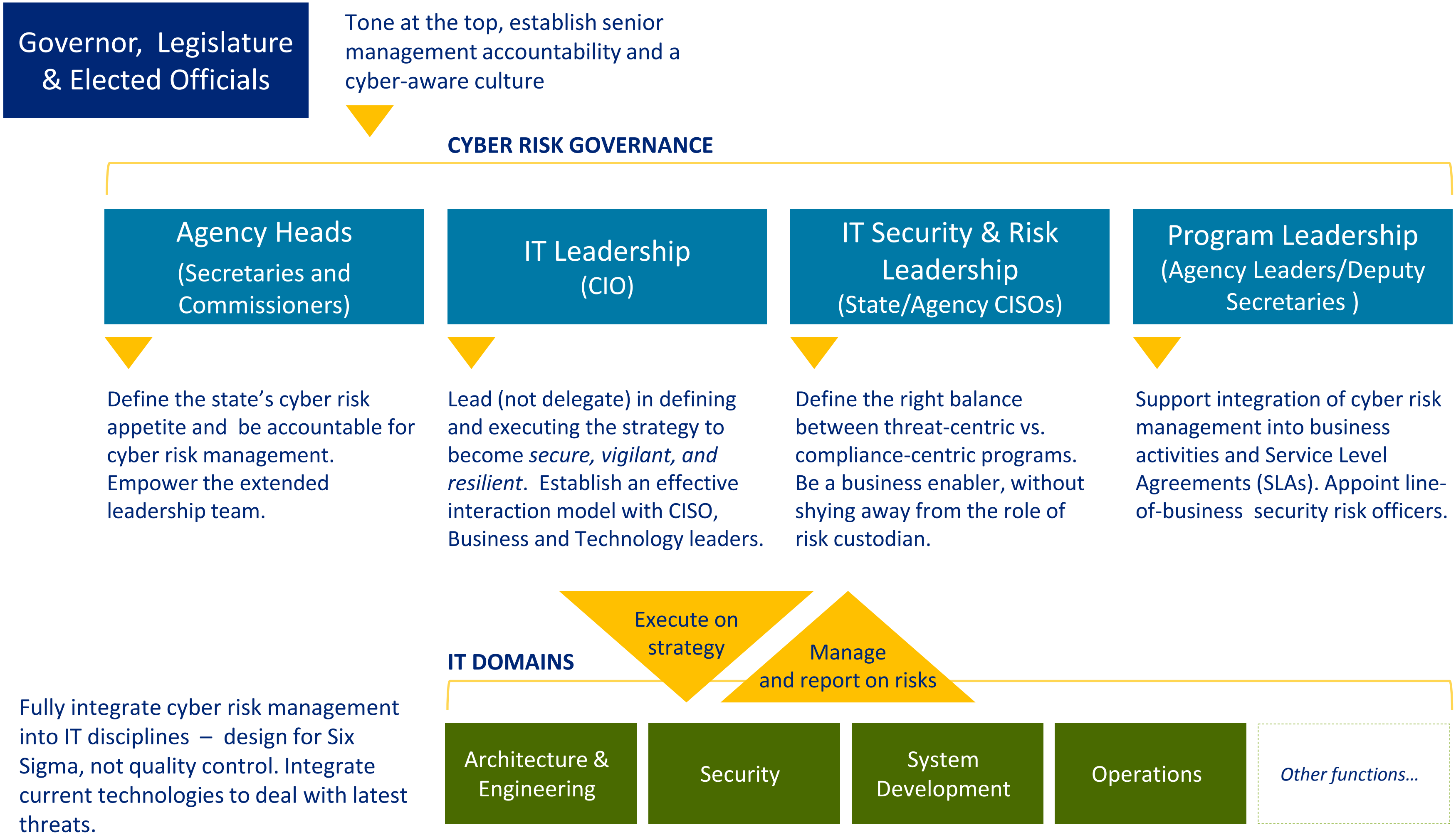
Sources:

[1] *http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2012.pdf*

[2] *"2011 Cost of Data Breach Study: Global." Ponemon Institute. March 2012.*

Executive sponsorship is the key to success

Every leader has a distinct role to play in driving alignment



Governor, Legislature & Elected Officials

Tone at the top, establish senior management accountability and a cyber-aware culture

CYBER RISK GOVERNANCE

Agency Heads (Secretaries and Commissioners)

Define the state's cyber risk appetite and be accountable for cyber risk management. Empower the extended leadership team.

IT Leadership (CIO)

Lead (not delegate) in defining and executing the strategy to become *secure, vigilant, and resilient*. Establish an effective interaction model with CISO, Business and Technology leaders.

IT Security & Risk Leadership (State/Agency CISOs)

Define the right balance between threat-centric vs. compliance-centric programs. Be a business enabler, without shying away from the role of risk custodian.

Program Leadership (Agency Leaders/Deputy Secretaries)

Support integration of cyber risk management into business activities and Service Level Agreements (SLAs). Appoint line-of-business security risk officers.

Execute on strategy

Manage and report on risks

IT DOMAINS

Fully integrate cyber risk management into IT disciplines – design for Six Sigma, not quality control. Integrate current technologies to deal with latest threats.

Architecture & Engineering

Security

System Development

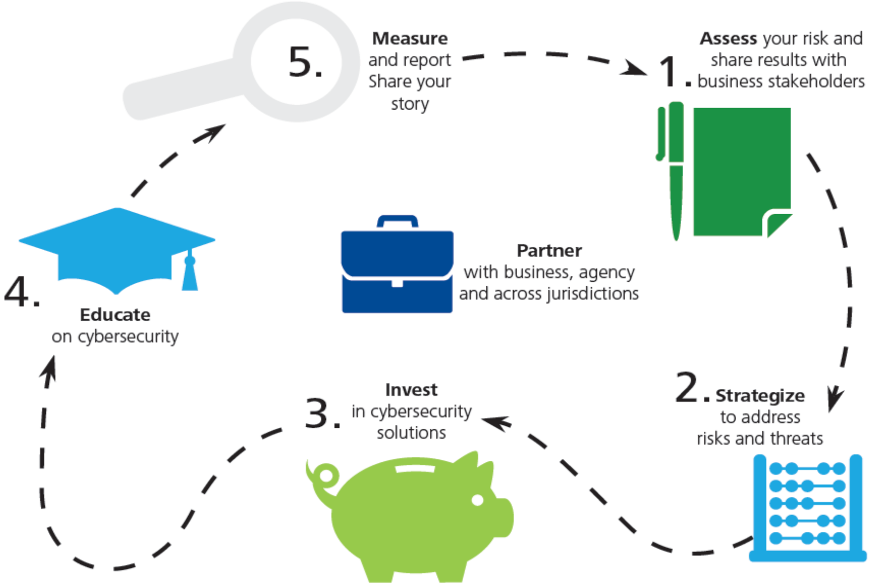
Operations

Other functions…

Cybersecurity – Planning to protect yourself

Actions for State Leadership

2012 Deloitte-NASCIO Cybersecurity study A call to action for States


5. Measure and report Share your story
1. Assess your risk and share results with business stakeholders
Partner with business, agency and across jurisdictions
4. Educate on cybersecurity
2. Strategize to address risks and threats
3. Invest in cybersecurity solutions

National Governors Association (NGA): "Act & Adjust" A Call to Action for Governors for Cybersecurity

- Establishing a governance and authority structure for cybersecurity.
- Conducting risk assessments and allocating resources accordingly.
- Implementing continuous vulnerability assessments and threat mitigation practices.
- Ensuring that the state complies with current security methodologies and business disciplines in cybersecurity.
- Creating a culture of risk awareness.

Planning & Management

- How do **we identify our critical assets** and associated risks and vulnerabilities?
- How do we meet **our critical infrastructure operations** and **regulatory requirements**?
- What is our **strategy and plan to protect our assets**?
- How broad and detailed are our **incident response and communication plans**?

Assets

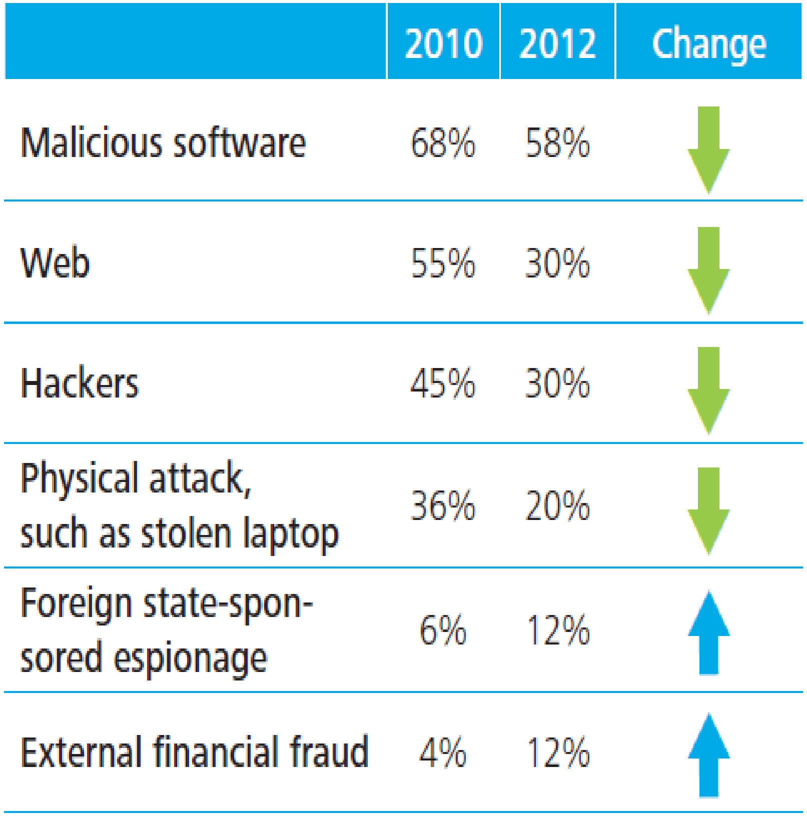
- How do we **track what digital information is leaving** our organization **and where** that information is going?
- How do we know **who's really logging into our network**, and from where?
- How do we control **what software is running** on our devices?
- **How do we limit the information** available to a cyber adversary?

Call for Action – Checklist of considerations

- ✓ Assess and communicate security risks.
- ✓ Better articulate risks and audit findings with business stakeholders.
- ✓ Explore creative paths to improve cybersecurity effectiveness within states' current federated governance models.
- ✓ Focus on audit and continuous monitoring of third-party compliance.
- ✓ Raise stakeholder awareness to combat accidental data breaches.
- ✓ Aggressively explore alternative funding sources including collaboration with other entities.
- ✓ Make better security an enabler of the use of emerging technologies.

Highlights from the NASCIO Study

The Changing Face of External Breaches (2010 vs. 2012)

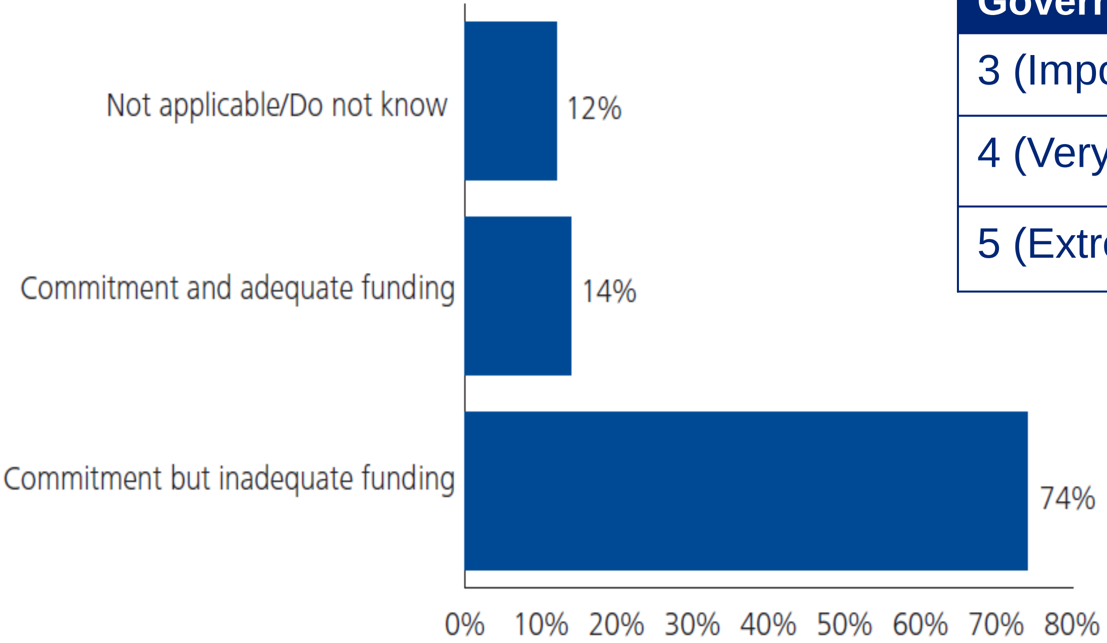


	2010	2012	Change
Malicious software	68%	58%	↓
Web	55%	30%	↓
Hackers	45%	30%	↓
Physical attack, such as stolen laptop	36%	20%	↓
Foreign state-sponsored espionage	6%	12%	↑
External financial fraud	4%	12%	↑

Emerging cybercrime and state-sponsored threats will require a strong response from states.

Highlights from the NASCIO Study (cont.)

Senior Executive Support for Security Projects to Address Legal/Regulatory Requirements

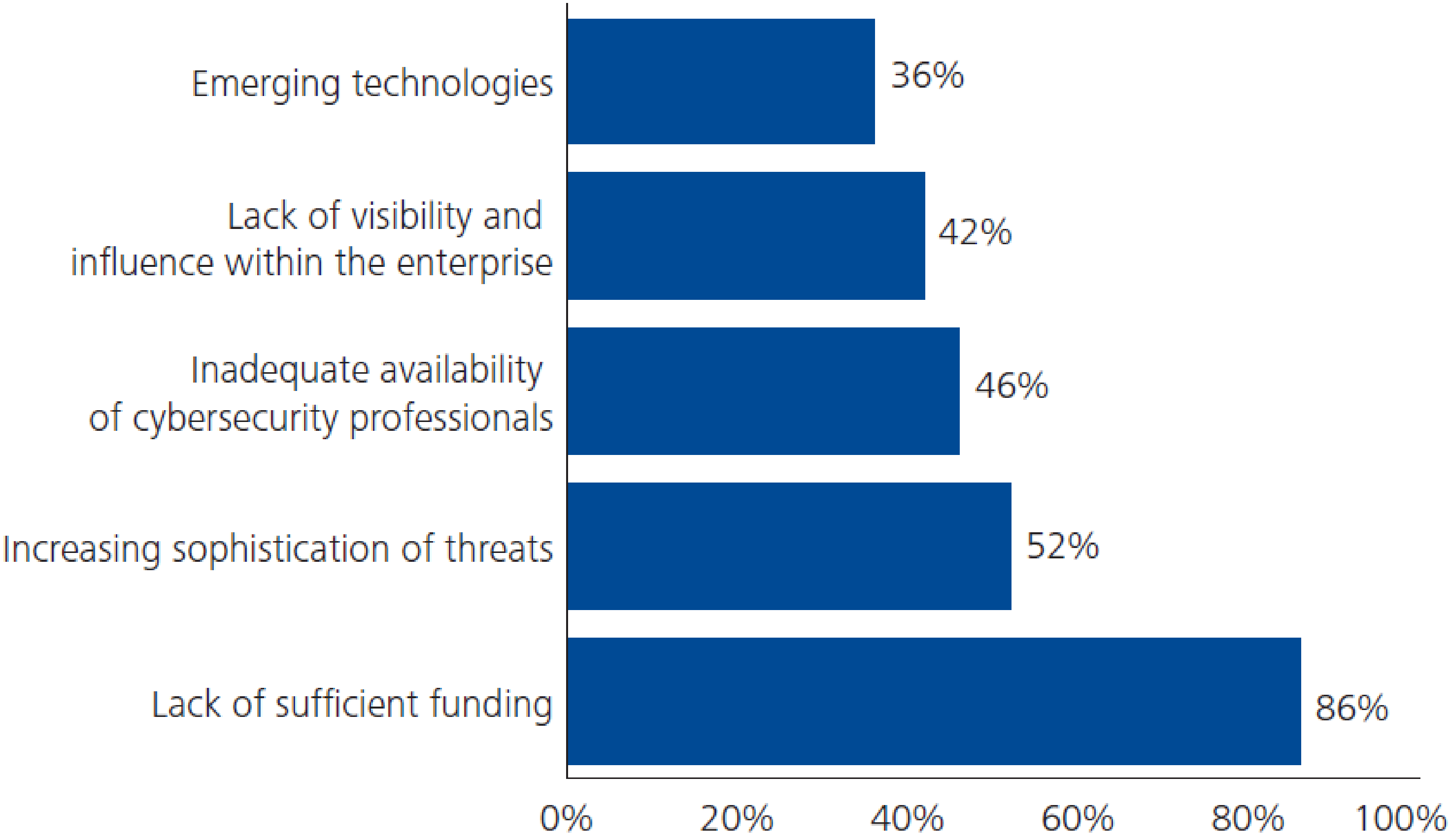


On a scale of 1 to 5, please indicate how you consider the importance of information security to your state Government?	
3 (Important)	7%
4 (Very Important)	11%
5 (Extremely Important)	81%

74% of CISO respondents have executive commitment—but that has not translated into adequate funding.

Highlights from the NASCIO Study (cont.)

Top Five Barriers faced in addressing Cybersecurity



Insufficient resources against growing sophistication of threats and emerging technologies make the need to raise stakeholder awareness to gain their support and funding the more critical.

Managing Cyber Risk

Questions