State Cybersecurity Update

Reducing Risk with the DoIT Risk Assessment Framework

SIAAB Fall Conference
October 26, 2016

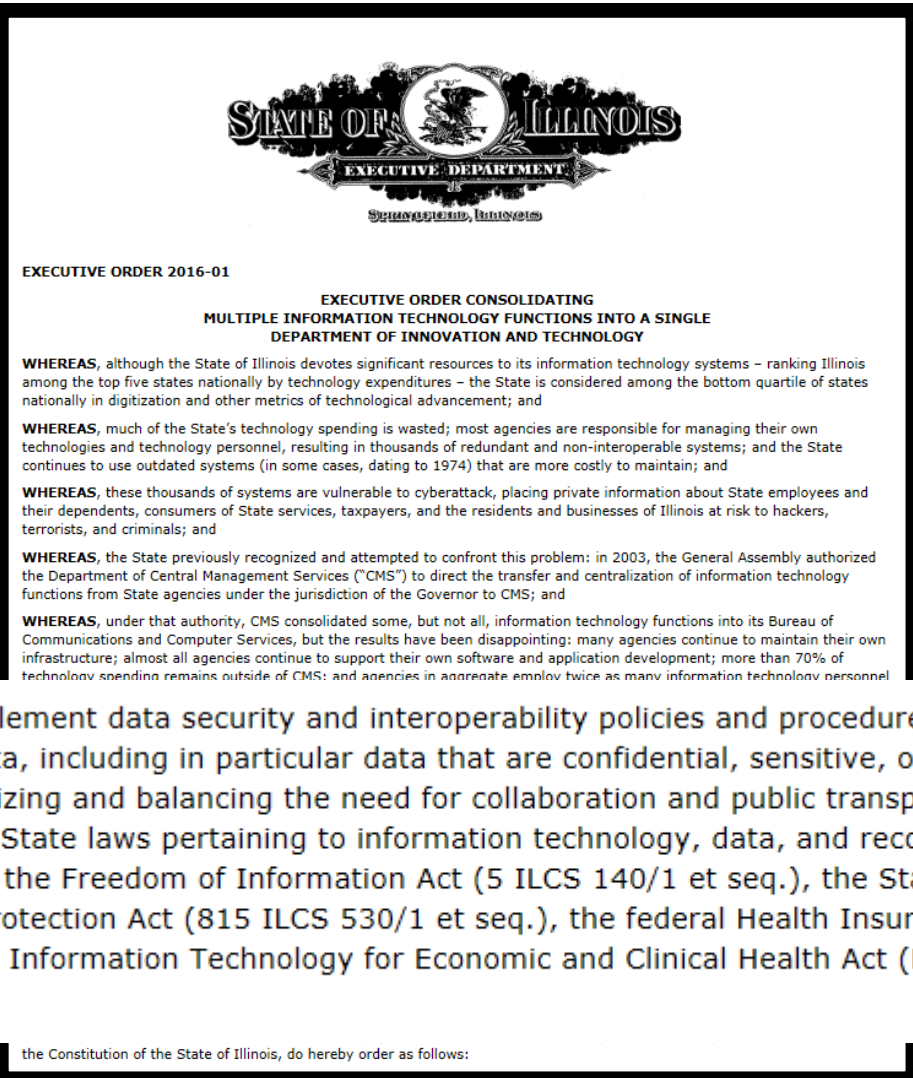
Introduction

Kirk Lonbom — Chief Information Security Officer, State of Illinois

- Responsible for information and cyber security for entities operating under the Governor
- 64 Agencies, Boards and Commissions
- 50,000 state employees
- Compliance areas including FISMA, HIPAA, PCI, CJIS, more

Our Charge

WHEREAS, these thousands of systems are vulnerable to cyberattack, placing private information about State employees and their dependents, consumers of State services, taxpayers, and the residents and businesses of Illinois at risk to hackers, terrorists, and criminals; and



STATE OF ILLINOIS
EXECUTIVE DEPARTMENT
Springfield, Illinois

EXECUTIVE ORDER 2016-01

EXECUTIVE ORDER CONSOLIDATING MULTIPLE INFORMATION TECHNOLOGY FUNCTIONS INTO A SINGLE DEPARTMENT OF INNOVATION AND TECHNOLOGY

WHEREAS, although the State of Illinois devotes significant resources to its information technology systems – ranking Illinois among the top five states nationally by technology expenditures – the State is considered among the bottom quartile of states nationally in digitization and other metrics of technological advancement; and

WHEREAS, much of the State's technology spending is wasted; most agencies are responsible for managing their own technologies and technology personnel, resulting in thousands of redundant and non-interoperable systems; and the State continues to use outdated systems (in some cases, dating to 1974) that are more costly to maintain; and

WHEREAS, these thousands of systems are vulnerable to cyberattack, placing private information about State employees and their dependents, consumers of State services, taxpayers, and the residents and businesses of Illinois at risk to hackers, terrorists, and criminals; and

WHEREAS, the State previously recognized and attempted to confront this problem: in 2003, the General Assembly authorized the Department of Central Management Services ("CMS") to direct the transfer and centralization of information technology functions from State agencies under the jurisdiction of the Governor to CMS; and

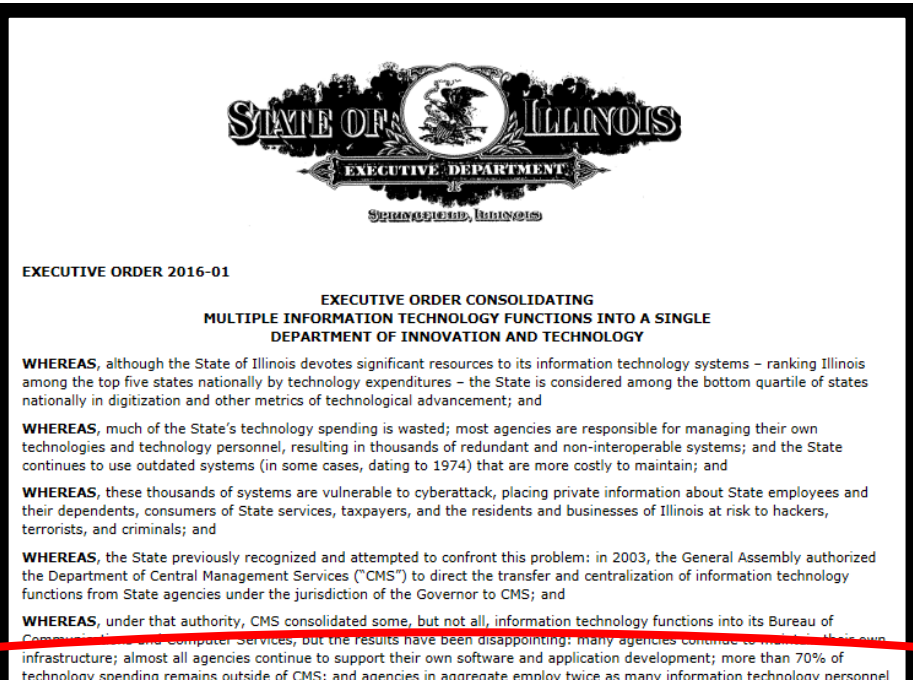
WHEREAS, under that authority, CMS consolidated some, but not all, information technology functions into its Bureau of Communications and Computer Services, but the results have been disappointing: many agencies continue to maintain their own infrastructure; almost all agencies continue to support their own software and application development; more than 70% of technology spending remains outside of CMS; and agencies in aggregate employ twice as many information technology personnel

the Constitution of the State of Illinois, do hereby order as follows:

DoIT shall develop and implement data security and interoperability policies and procedures that ensure the security and interoperability of State data, including in particular data that are confidential, sensitive, or protected from disclosure by privacy or other laws, while recognizing and balancing the need for collaboration and public transparency. DoIT shall ensure compliance with applicable federal and State laws pertaining to information technology, data, and records of DoIT and the client agencies, including without limitation the Freedom of Information Act (5 ILCS 140/1 et seq.), the State Records Act (5 ILCS 160/1 et seq.), the Personal Information Protection Act (815 ILCS 530/1 et seq.), the federal Health Insurance Portability and Accountability Act (HIPAA), the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the federal Gramm-Leach-Bliley Act.

Our Charge

WHEREAS, these thousands of systems are vulnerable to cyberattack, placing private information about State employees and their dependents, consumers of State services, taxpayers, and the residents and businesses of Illinois at risk to hackers, terrorists, and criminals; and



STATE OF ILLINOIS
EXECUTIVE DEPARTMENT
Springfield, Illinois

EXECUTIVE ORDER 2016-01

EXECUTIVE ORDER CONSOLIDATING MULTIPLE INFORMATION TECHNOLOGY FUNCTIONS INTO A SINGLE DEPARTMENT OF INNOVATION AND TECHNOLOGY

WHEREAS, although the State of Illinois devotes significant resources to its information technology systems – ranking Illinois among the top five states nationally by technology expenditures – the State is considered among the bottom quartile of states nationally in digitization and other metrics of technological advancement; and

WHEREAS, much of the State's technology spending is wasted; most agencies are responsible for managing their own technologies and technology personnel, resulting in thousands of redundant and non-interoperable systems; and the State continues to use outdated systems (in some cases, dating to 1974) that are more costly to maintain; and

WHEREAS, these thousands of systems are vulnerable to cyberattack, placing private information about State employees and their dependents, consumers of State services, taxpayers, and the residents and businesses of Illinois at risk to hackers, terrorists, and criminals; and

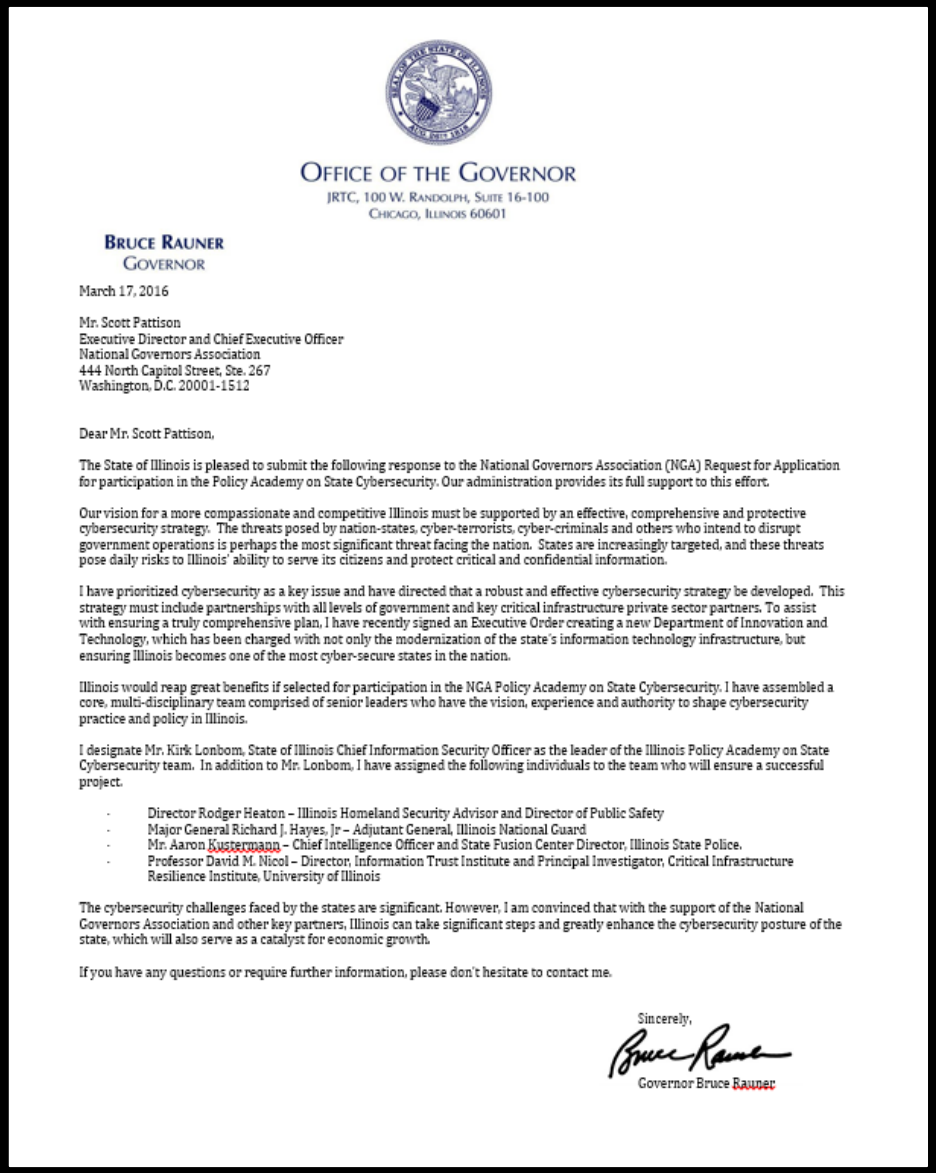
WHEREAS, the State previously recognized and attempted to confront this problem: in 2003, the General Assembly authorized the Department of Central Management Services ("CMS") to direct the transfer and centralization of information technology functions from State agencies under the jurisdiction of the Governor to CMS; and

WHEREAS, under that authority, CMS consolidated some, but not all, information technology functions into its Bureau of Communication and Computer Services, but the results have been disappointing: many agencies continue to maintain their own infrastructure; almost all agencies continue to support their own software and application development; more than 70% of technology spending remains outside of CMS; and agencies in aggregate employ twice as many information technology personnel

DoIT shall develop and implement data security and interoperability policies and procedures that ensure the security and interoperability of State data, including in particular data that are confidential, sensitive, or protected from disclosure by privacy or other laws, while recognizing and balancing the need for collaboration and public transparency. DoIT shall ensure compliance with applicable federal and State laws pertaining to information technology, data, and records of DoIT and the client agencies, including without limitation the Freedom of Information Act (5 ILCS 140/1 et seq.), the State Records Act (5 ILCS 160/1 et seq.), the Personal Information Protection Act (815 ILCS 530/1 et seq.), the federal Health Insurance Portability and Accountability Act (HIPAA), the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the federal Gramm-Leach-Bliley Act.

the Constitution of the State of Illinois, do hereby order as follows:

Our Charge



OFFICE OF THE GOVERNOR
JRTC, 100 W. RANDOLPH, SUITE 16-100
CHICAGO, ILLINOIS 60601

BRUCE RAUNER
GOVERNOR

March 17, 2016

Mr. Scott Pattison
Executive Director and Chief Executive Officer
National Governors Association
444 North Capitol Street, Ste. 267
Washington, D.C. 20001-1512

Dear Mr. Scott Pattison,

The State of Illinois is pleased to submit the following response to the National Governors Association (NGA) Request for Application for participation in the Policy Academy on State Cybersecurity. Our administration provides its full support to this effort.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy. The threats posed by nation-states, cyber-terrorists, cyber-criminals and others who intend to disrupt government operations is perhaps the most significant threat facing the nation. States are increasingly targeted, and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information.

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed. This strategy must include partnerships with all levels of government and key critical infrastructure private sector partners. To assist with ensuring a truly comprehensive plan, I have recently signed an Executive Order creating a new Department of Innovation and Technology, which has been charged with not only the modernization of the state's information technology infrastructure, but ensuring Illinois becomes one of the most cyber-secure states in the nation.

Illinois would reap great benefits if selected for participation in the NGA Policy Academy on State Cybersecurity. I have assembled a core, multi-disciplinary team comprised of senior leaders who have the vision, experience and authority to shape cybersecurity practice and policy in Illinois.

I designate Mr. Kirk Lonbom, State of Illinois Chief Information Security Officer as the leader of the Illinois Policy Academy on State Cybersecurity team. In addition to Mr. Lonbom, I have assigned the following individuals to the team who will ensure a successful project.

- Director Rodger Heaton – Illinois Homeland Security Advisor and Director of Public Safety
- Major General Richard J. Hayes, Jr – Adjutant General, Illinois National Guard
- Mr. Aaron Kustermann – Chief Intelligence Officer and State Fusion Center Director, Illinois State Police.
- Professor David M. Nicol – Director, Information Trust Institute and Principal Investigator, Critical Infrastructure Resilience Institute, University of Illinois

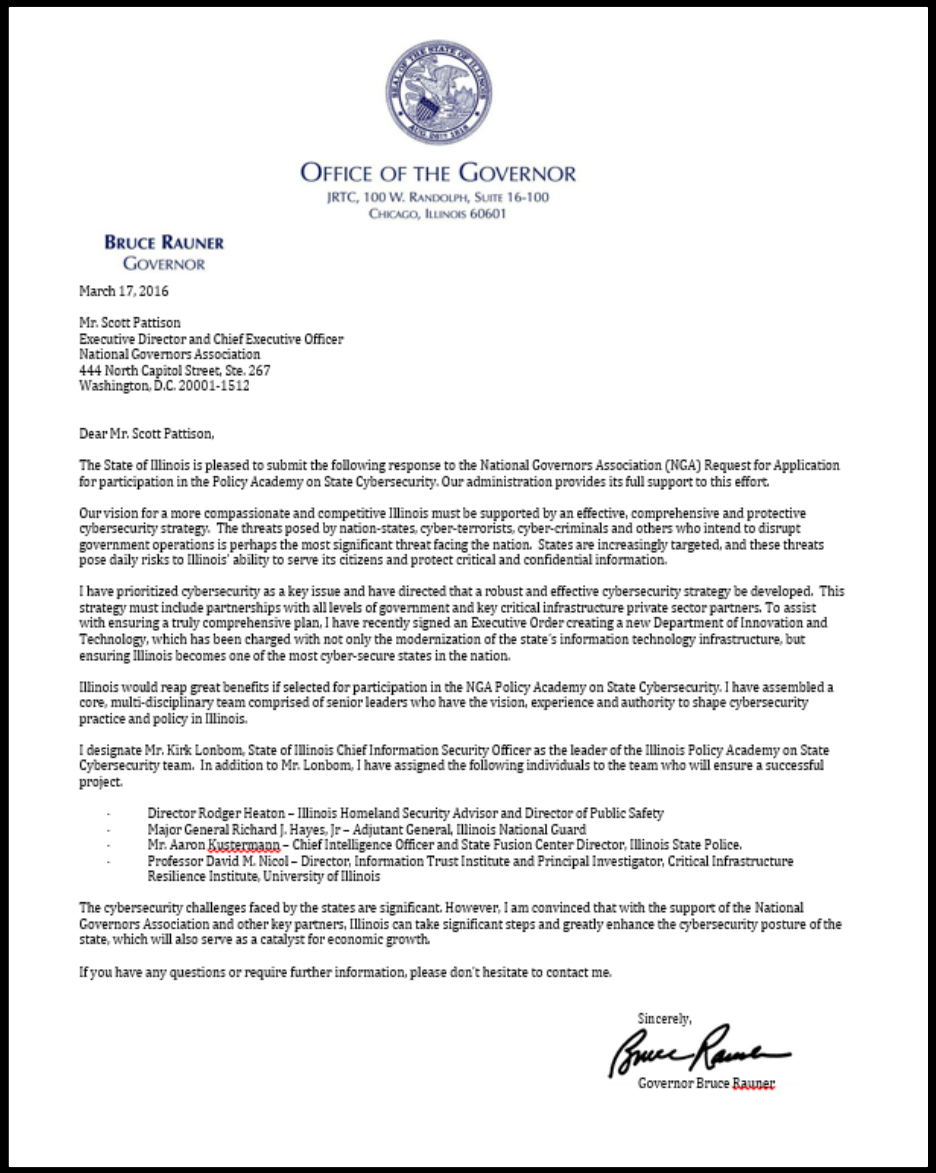
The cybersecurity challenges faced by the states are significant. However, I am convinced that with the support of the National Governors Association and other key partners, Illinois can take significant steps and greatly enhance the cybersecurity posture of the state, which will also serve as a catalyst for economic growth.

If you have any questions or require further information, please don't hesitate to contact me.

Sincerely,

Governor Bruce Rauner

Our Charge



OFFICE OF THE GOVERNOR
JRTC, 100 W. RANDOLPH, SUITE 16-100
CHICAGO, ILLINOIS 60601

BRUCE RAUNER
GOVERNOR

March 17, 2016

Mr. Scott Pattison
Executive Director and Chief Executive Officer
National Governors Association
444 North Capitol Street, Ste. 267
Washington, D.C. 20001-1512

Dear Mr. Scott Pattison,

The State of Illinois is pleased to submit the following response to the National Governors Association (NGA) Request for Application for participation in the Policy Academy on State Cybersecurity. Our administration provides its full support to this effort.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy. The threats posed by nation-states, cyber-terrorists, cyber-criminals and others who intend to disrupt government operations is perhaps the most significant threat facing the nation. States are increasingly targeted, and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information.

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed. This strategy must include partnerships with all levels of government and key critical infrastructure private sector partners. To assist with ensuring a truly comprehensive plan, I have recently signed an Executive Order creating a new Department of Innovation and Technology, which has been charged with not only the modernization of the state's information technology infrastructure, but ensuring Illinois becomes one of the most cyber-secure states in the nation.

Illinois would reap great benefits if selected for participation in the NGA Policy Academy on State Cybersecurity. I have assembled a core, multi-disciplinary team comprised of senior leaders who have the vision, experience and authority to shape cybersecurity practice and policy in Illinois.

I designate Mr. Kirk Lonbom, State of Illinois Chief Information Security Officer as the leader of the Illinois Policy Academy on State Cybersecurity team. In addition to Mr. Lonbom, I have assigned the following individuals to the team who will ensure a successful project.

- Director Rodger Heaton – Illinois Homeland Security Advisor and Director of Public Safety
- Major General Richard J. Hayes, Jr – Adjutant General, Illinois National Guard
- Mr. Aaron Kustermann – Chief Intelligence Officer and State Fusion Center Director, Illinois State Police.
- Professor David M. Nicol – Director, Information Trust Institute and Principal Investigator, Critical Infrastructure Resilience Institute, University of Illinois

The cybersecurity challenges faced by the states are significant. However, I am convinced that with the support of the National Governors Association and other key partners, Illinois can take significant steps and greatly enhance the cybersecurity posture of the state, which will also serve as a catalyst for economic growth.

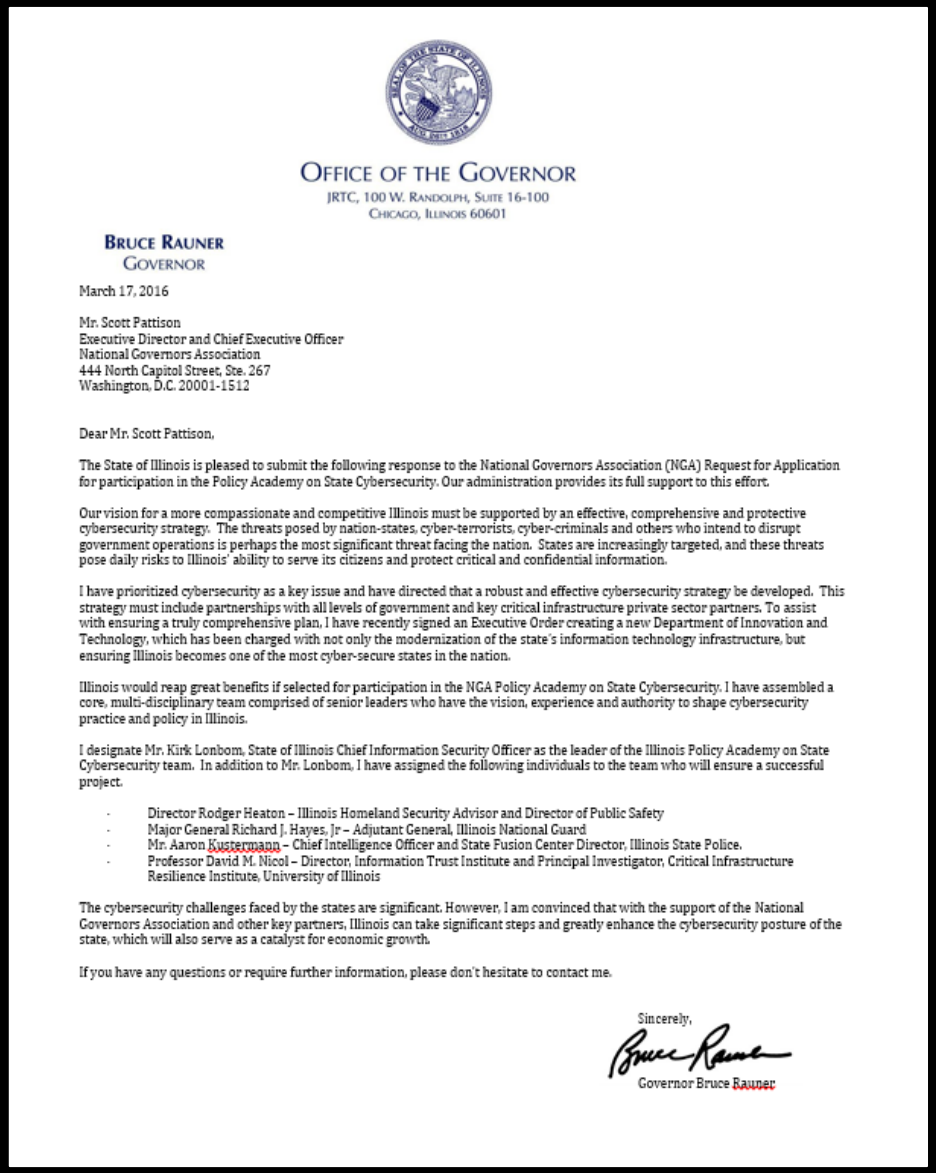
If you have any questions or require further information, please don't hesitate to contact me.

Sincerely,

Governor Bruce Rauner

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed.

Our Charge



OFFICE OF THE GOVERNOR
JRTC, 100 W. RANDOLPH, SUITE 16-100
CHICAGO, ILLINOIS 60601

BRUCE RAUNER
GOVERNOR

March 17, 2016

Mr. Scott Pattison
Executive Director and Chief Executive Officer
National Governors Association
444 North Capitol Street, Ste. 267
Washington, D.C. 20001-1512

Dear Mr. Scott Pattison,

The State of Illinois is pleased to submit the following response to the National Governors Association (NGA) Request for Application for participation in the Policy Academy on State Cybersecurity. Our administration provides its full support to this effort.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy. The threats posed by nation-states, cyber-terrorists, cyber-criminals and others who intend to disrupt government operations is perhaps the most significant threat facing the nation. States are increasingly targeted, and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information.

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed. This strategy must include partnerships with all levels of government and key critical infrastructure private sector partners. To assist with ensuring a truly comprehensive plan, I have recently signed an Executive Order creating a new Department of Innovation and Technology, which has been charged with not only the modernization of the state's information technology infrastructure, but ensuring Illinois becomes one of the most cyber-secure states in the nation.

Illinois would reap great benefits if selected for participation in the NGA Policy Academy on State Cybersecurity. I have assembled a core, multi-disciplinary team comprised of senior leaders who have the vision, experience and authority to shape cybersecurity practice and policy in Illinois.

I designate Mr. Kirk Lonbom, State of Illinois Chief Information Security Officer as the leader of the Illinois Policy Academy on State Cybersecurity team. In addition to Mr. Lonbom, I have assigned the following individuals to the team who will ensure a successful project.

- Director Rodger Heaton – Illinois Homeland Security Advisor and Director of Public Safety
- Major General Richard J. Hayes, Jr – Adjutant General, Illinois National Guard
- Mr. Aaron Kustermann – Chief Intelligence Officer and State Fusion Center Director, Illinois State Police.
- Professor David M. Nicol – Director, Information Trust Institute and Principal Investigator, Critical Infrastructure Resilience Institute, University of Illinois

The cybersecurity challenges faced by the states are significant. However, I am convinced that with the support of the National Governors Association and other key partners, Illinois can take significant steps and greatly enhance the cybersecurity posture of the state, which will also serve as a catalyst for economic growth.

If you have any questions or require further information, please don't hesitate to contact me.

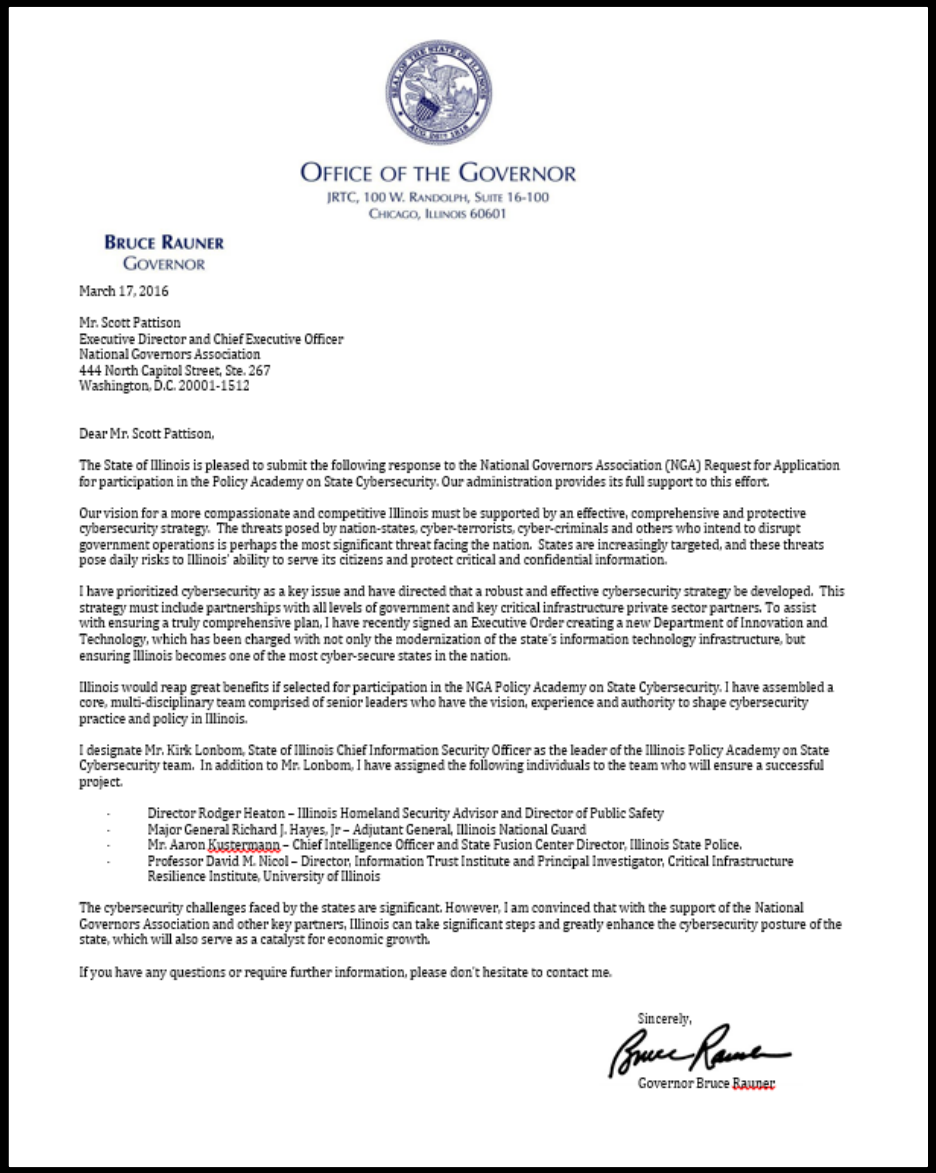
Sincerely,

Governor Bruce Rauner

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy.

Our Charge



OFFICE OF THE GOVERNOR
JRTC, 100 W. RANDOLPH, SUITE 16-100
CHICAGO, ILLINOIS 60601

BRUCE RAUNER
GOVERNOR

March 17, 2016

Mr. Scott Pattison
Executive Director and Chief Executive Officer
National Governors Association
444 North Capitol Street, Ste. 267
Washington, D.C. 20001-1512

Dear Mr. Scott Pattison,

The State of Illinois is pleased to submit the following response to the National Governors Association (NGA) Request for Application for participation in the Policy Academy on State Cybersecurity. Our administration provides its full support to this effort.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy. The threats posed by nation-states, cyber-terrorists, cyber-criminals and others who intend to disrupt government operations is perhaps the most significant threat facing the nation. States are increasingly targeted, and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information.

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed. This strategy must include partnerships with all levels of government and key critical infrastructure private sector partners. To assist with ensuring a truly comprehensive plan, I have recently signed an Executive Order creating a new Department of Innovation and Technology, which has been charged with not only the modernization of the state's information technology infrastructure, but ensuring Illinois becomes one of the most cyber-secure states in the nation.

Illinois would reap great benefits if selected for participation in the NGA Policy Academy on State Cybersecurity. I have assembled a core, multi-disciplinary team comprised of senior leaders who have the vision, experience and authority to shape cybersecurity practice and policy in Illinois.

I designate Mr. Kirk Lonbom, State of Illinois Chief Information Security Officer as the leader of the Illinois Policy Academy on State Cybersecurity team. In addition to Mr. Lonbom, I have assigned the following individuals to the team who will ensure a successful project.

- Director Rodger Heaton – Illinois Homeland Security Advisor and Director of Public Safety
- Major General Richard J. Hayes, Jr – Adjutant General, Illinois National Guard
- Mr. Aaron Kustermann – Chief Intelligence Officer and State Fusion Center Director, Illinois State Police.
- Professor David M. Nicol – Director, Information Trust Institute and Principal Investigator, Critical Infrastructure Resilience Institute, University of Illinois

The cybersecurity challenges faced by the states are significant. However, I am convinced that with the support of the National Governors Association and other key partners, Illinois can take significant steps and greatly enhance the cybersecurity posture of the state, which will also serve as a catalyst for economic growth.

If you have any questions or require further information, please don't hesitate to contact me.

Sincerely,

Governor Bruce Rauner

I have prioritized cybersecurity as a key issue and have directed that a robust and effective cybersecurity strategy be developed.

Our vision for a more compassionate and competitive Illinois must be supported by an effective, comprehensive and protective cybersecurity strategy.

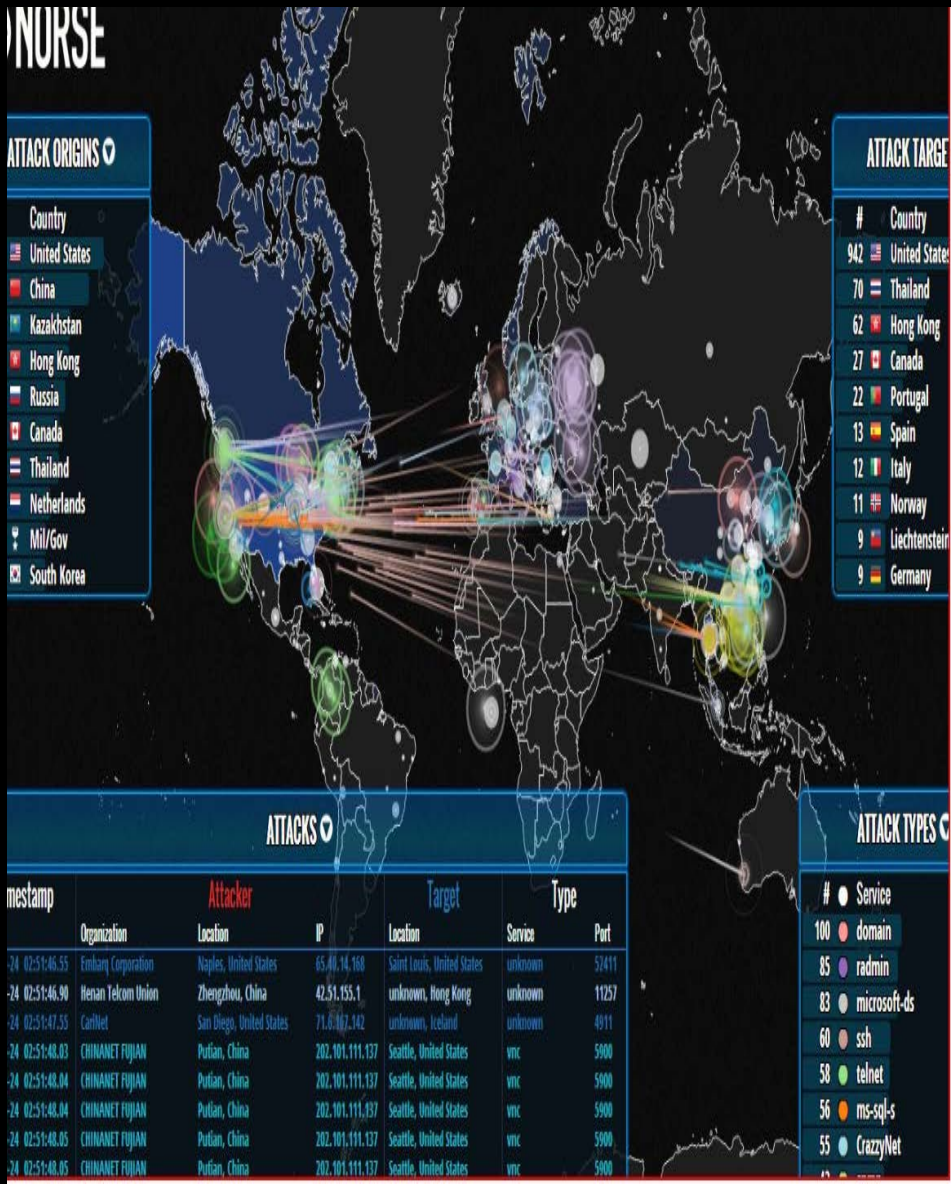
This strategy must include partnerships with all levels of government and key critical infrastructure private sector partners.

Sincerely,

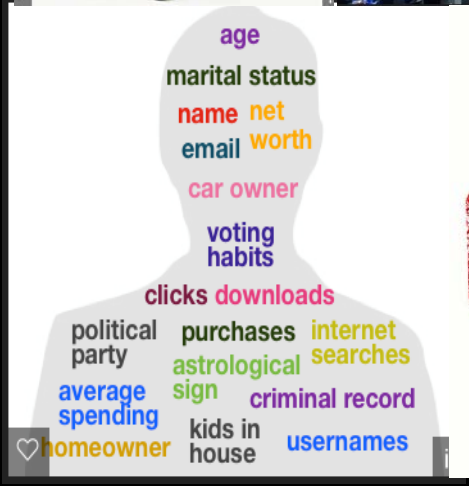
Governor Bruce Rauner

What is the current situation?

- The State of Illinois is under constant attack
- Attacks against states are rising
- Attacks are increasing in intensity
- Various levels of security practices across state agencies
- Working to better protect the state from the threat

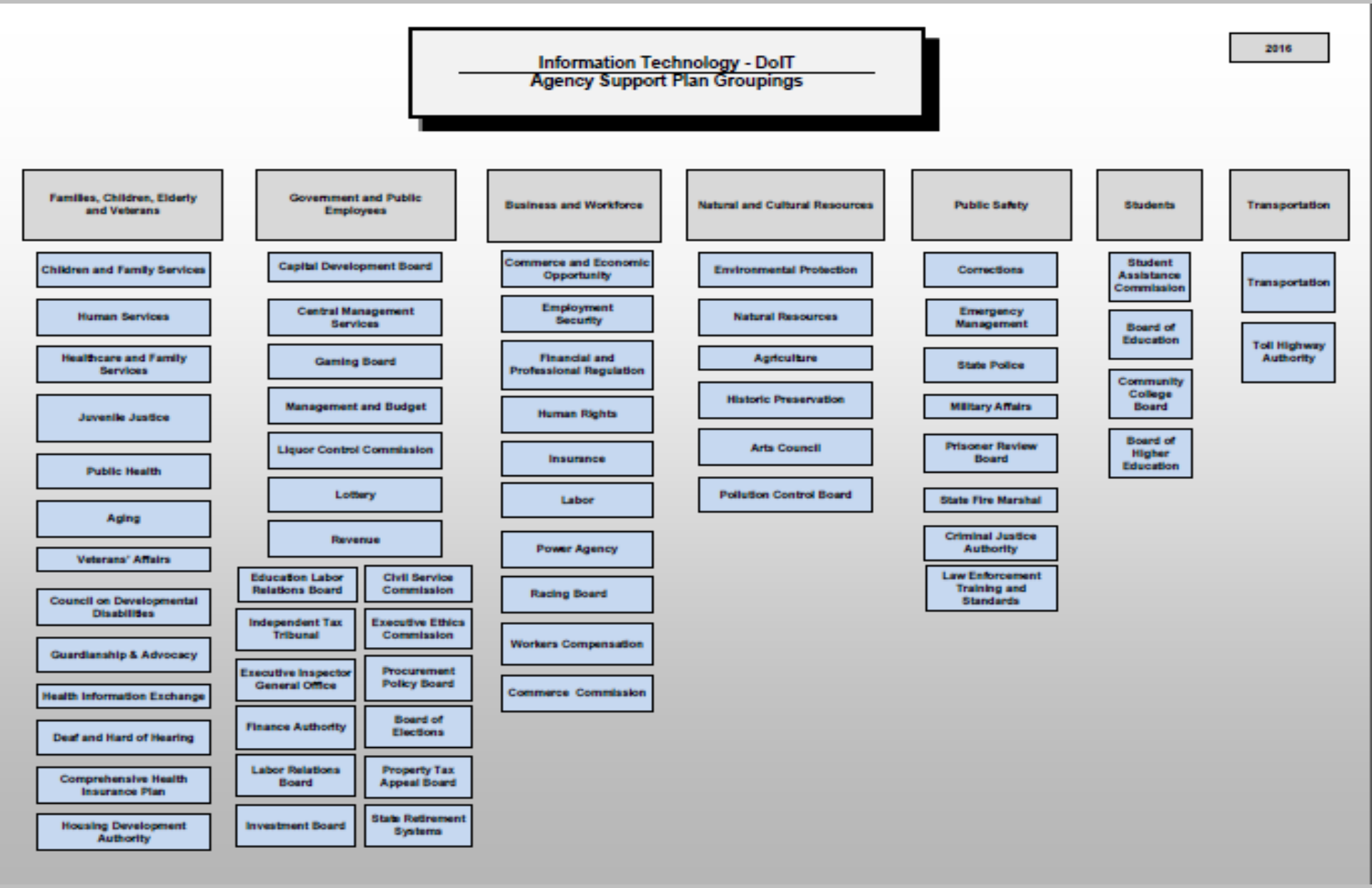


What is the current situation?



- Critical life, health and safety systems must be available
  - Public Safety
  - Crucial Services to Citizens
- The State holds billions of confidential records
  - PII
  - PHI
  - Intelligence
  - Other Confidential
- Information integrity must be maintained
- We must be able to withstand and recover.

Our Challenge



Security is an Executive Level Matter

RISK is an Executive Level Matter

RISK is an Executive Level Matter

RISK ACCEPTANCE IS A BUSINESS DECISION TO BE MADE AT THE EXECUTIVE LEVEL

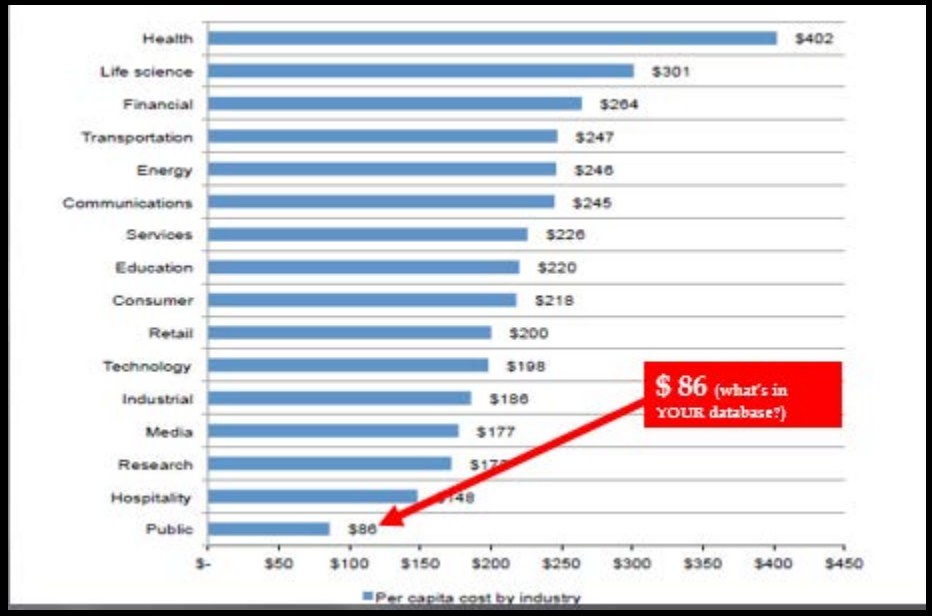
(NOT BY I.T.)

What DO we care about?

- State Business Risk
  - Life, Health and Safety
  - Delivering Services to our Citizens
  - Delivering Services to our Employees

What DO we care about?

- State Business Risk
  - Life, Health and Safety
  - Delivering Services to our Citizens
  - Delivering Services to our Employees
- Financial Risk
  - Lost Revenue
  - Breach Costs
  - Fraud and Theft



What DO we care about?

- State Business Risk
  - Life, Health and Safety
  - Delivering Services to our Citizens
  - Delivering Services to our Employees
- Financial Risk
  - Lost Revenue
  - Breach Costs
  - Fraud and Theft
- Privacy & Confidentiality Risk
  - Personal Information – Identify Theft
  - Confidential Information

What DO we care about?

- State Business Risk
  - Life, Health and Safety
  - Delivering Services to our Citizens
  - Delivering Services to our Employees
- Financial Risk
  - Lost Revenue
  - Breach Costs
  - Fraud and Theft
- Privacy & Confidentiality Risk
  - Personal Information – Identify Theft
  - Confidential Information
- Reputational/Political Risk
  - Elected Officials
  - Agency Directors
  - Program Managers

Goals

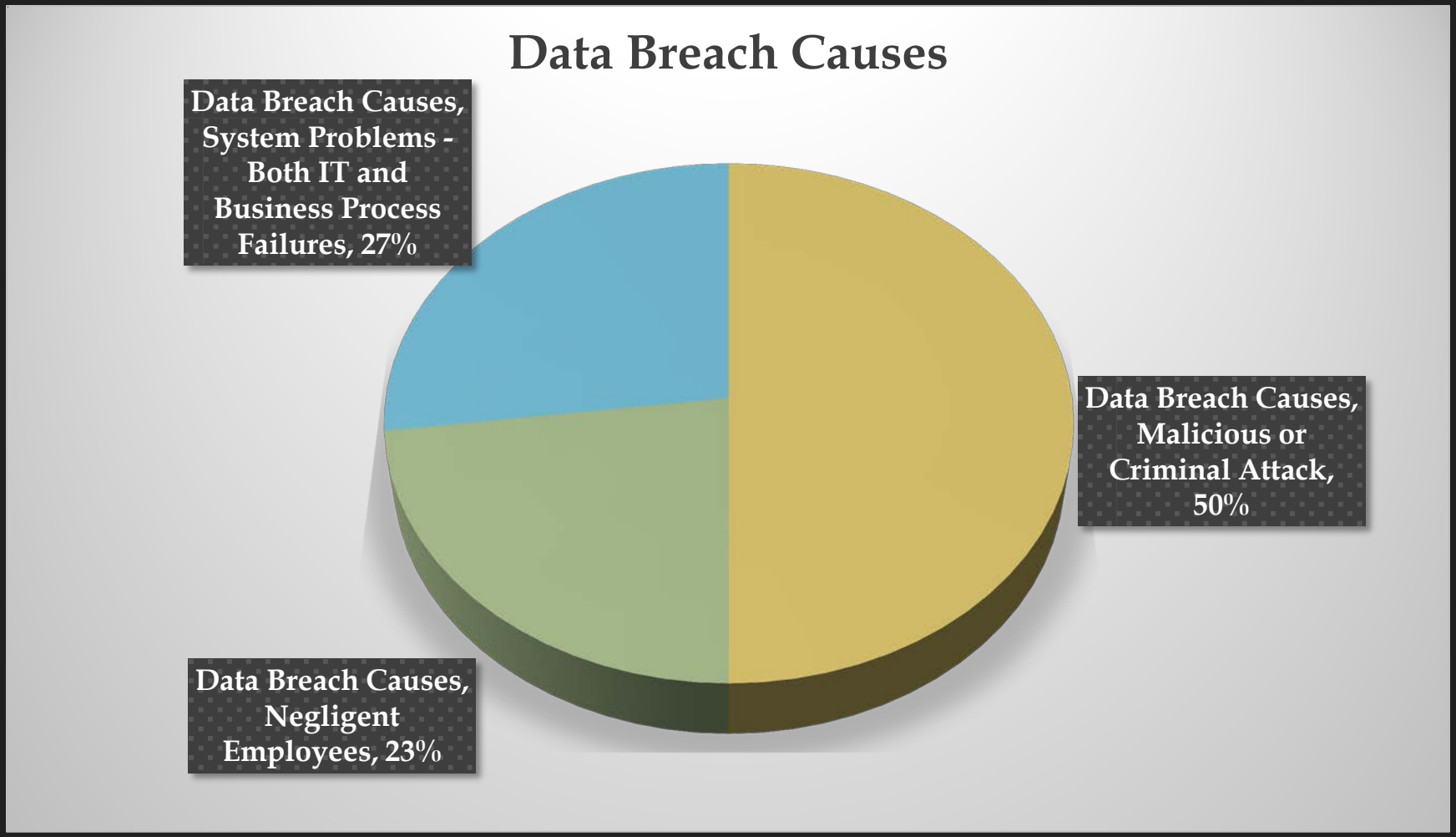
- Information Security
  - Protect information from unauthorized disclosure
  - Ensure information is trustworthy
  - Guarantee reliable access to mission critical information

- Cyber-Resiliency
  - Ability to anticipate, withstand and recover from adverse cyber-events.
  - Evolve and improve in pace with the ever-changing cyber landscape.

2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

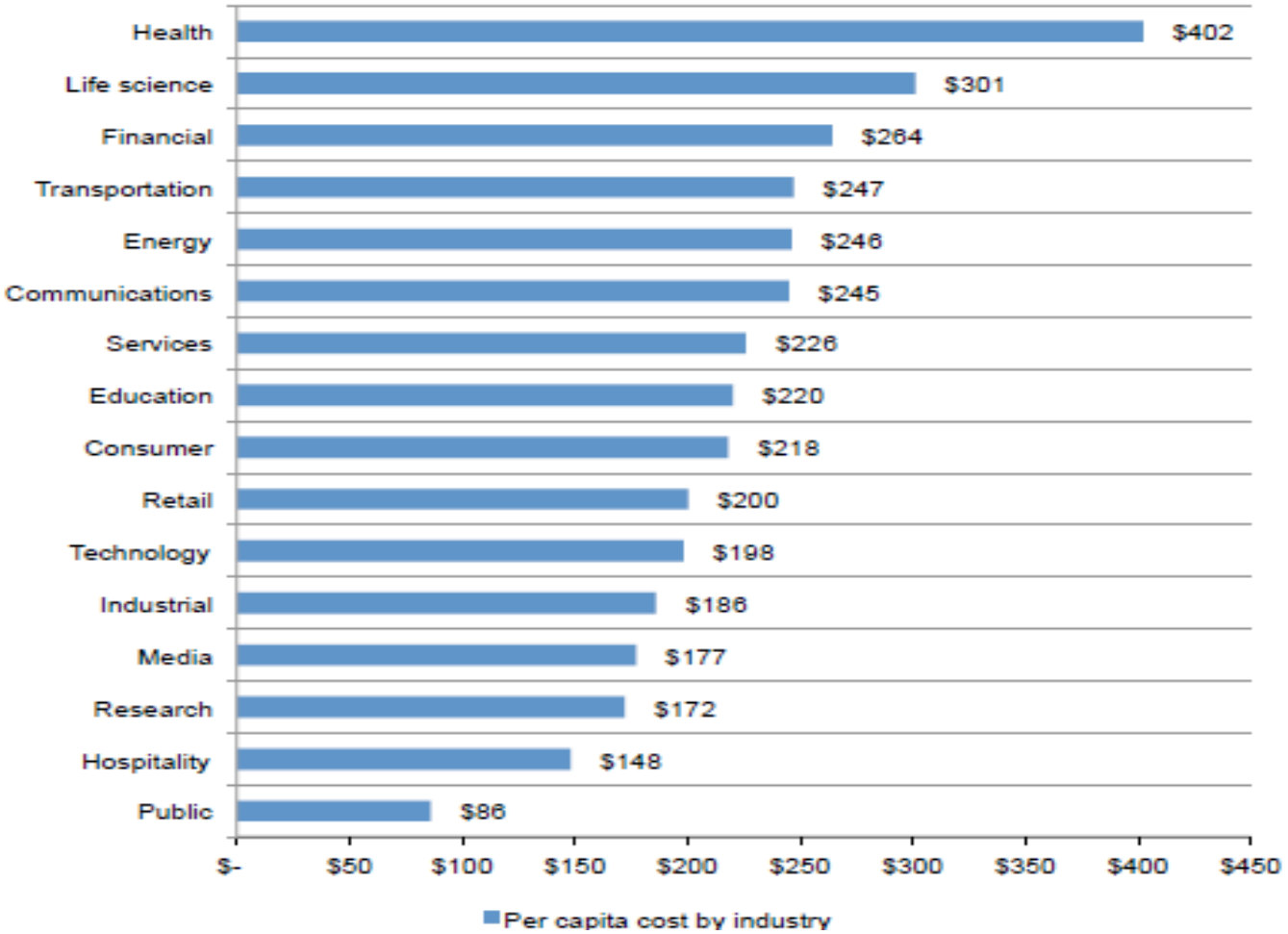
Primary Causes of Data Breaches



Breach Costs Are Rising

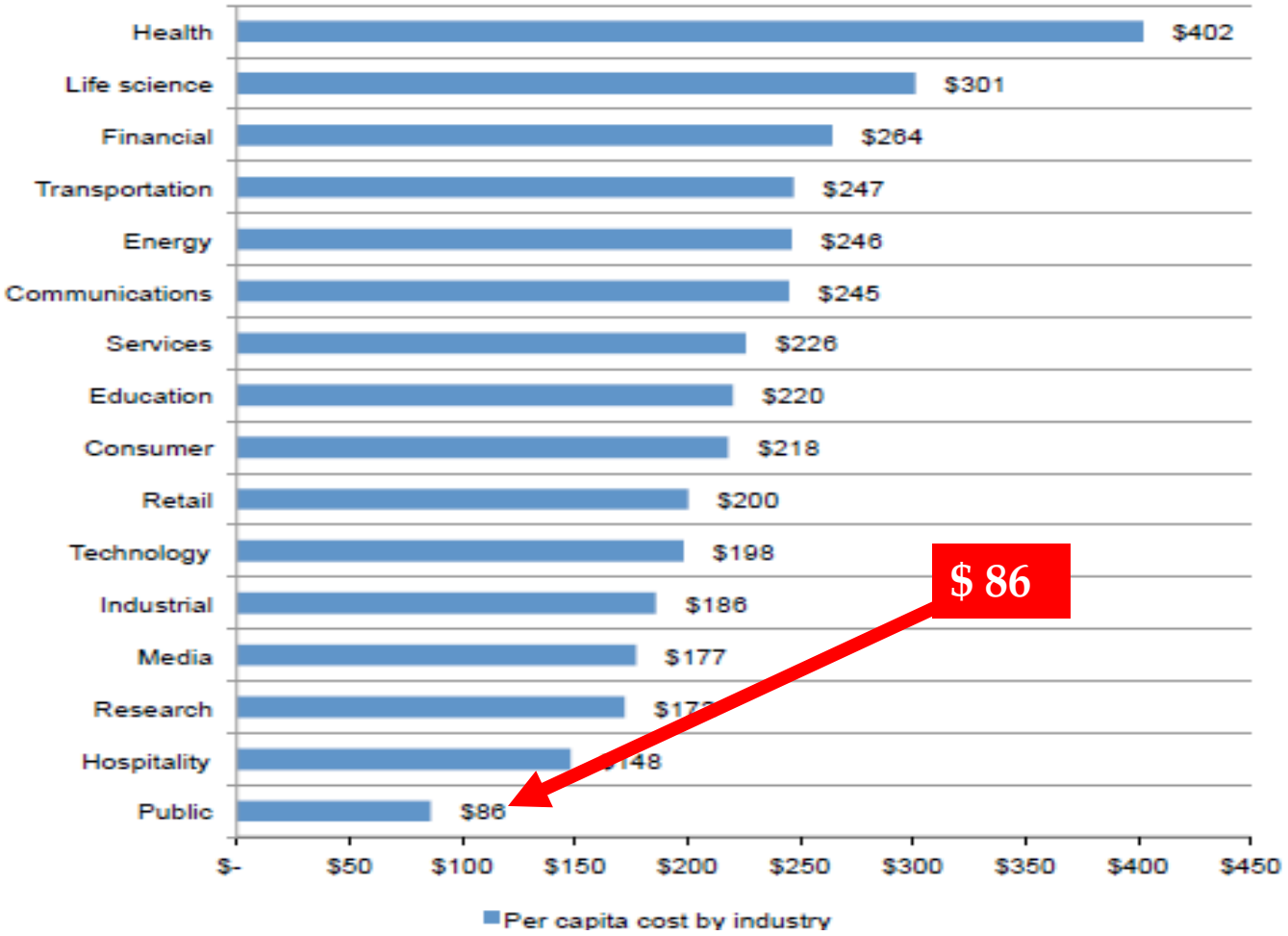
Breach Costs- Per Record

(From IBM-Ponemon Study)



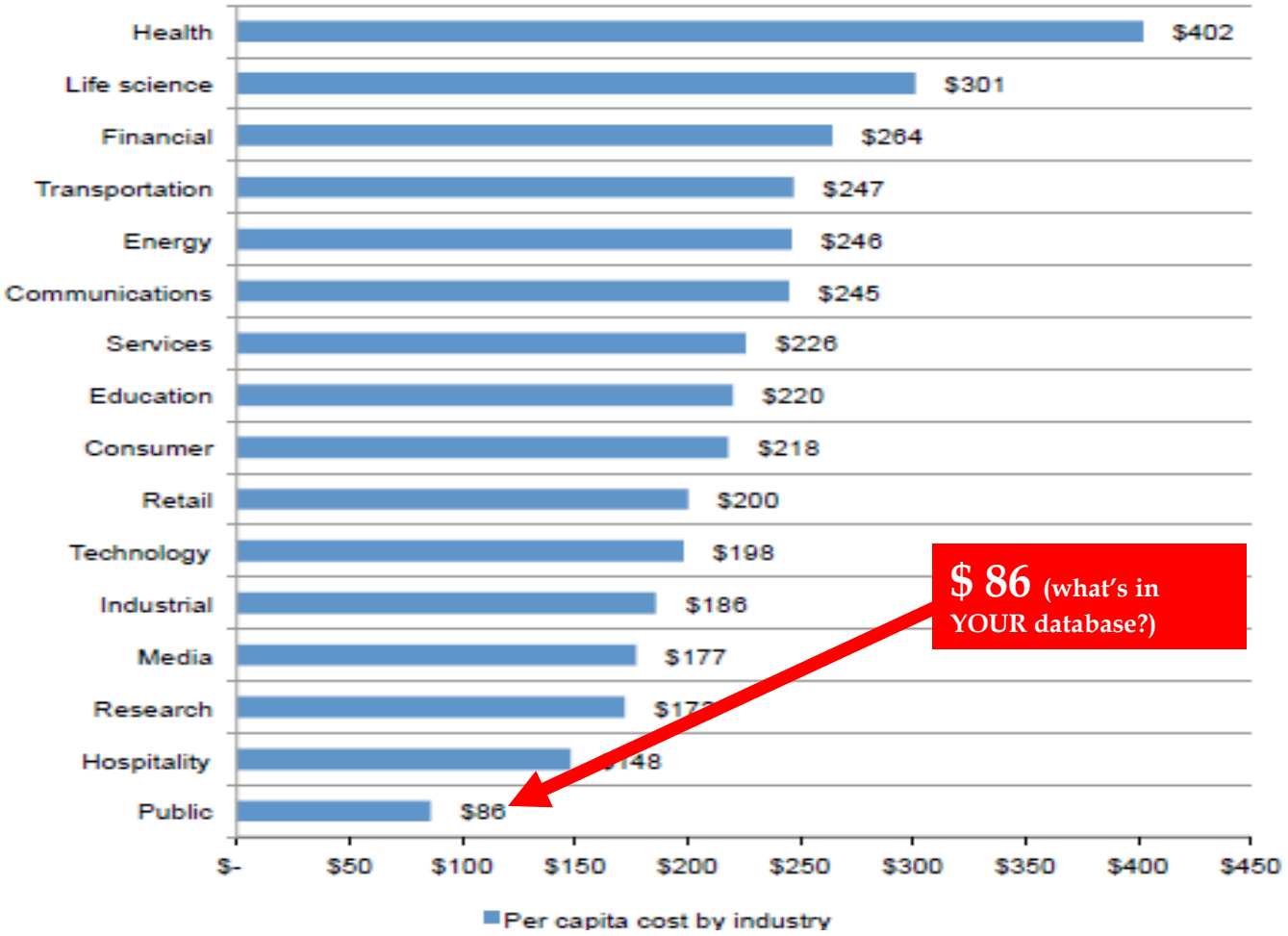
Breach Costs- Per Record

(From IBM-Ponemon Study)



Breach Costs- Per Record

(From IBM-Ponemon Study)



What are WE seeing?

- Daily Phishing, Brute Force, Calls, SQLi
- Ransomware
- DDos Attacks – States and Law Enforcement
- Insider Concerns
- Indications of Increased Nation State Activity

What are WE seeing?

CNN politics

Search CNN ...

Election 2016 Nation World Our Team

Officials: Hackers breach election systems in Illinois, Arizona

By **Wesley Bruer** and **Evan Perez**, CNN
Updated 2:08 PM ET, Tue August 30, 2016

What are WE seeing?

The New York Times

Europe

SUBSCRIBE | LOG IN

A Voice Cuts Through, and Adds to, the Intrigue of Russia's Cyberattacks

Vladimir M. Fomenko in Biysk, Russia. Mr. Fomenko is the owner of King Servers, which rents server space, including to those implicated in recent hacking attempts on election systems in Arizona and Illinois.
BRENDAN HOFFMAN FOR THE NEW YORK TIMES

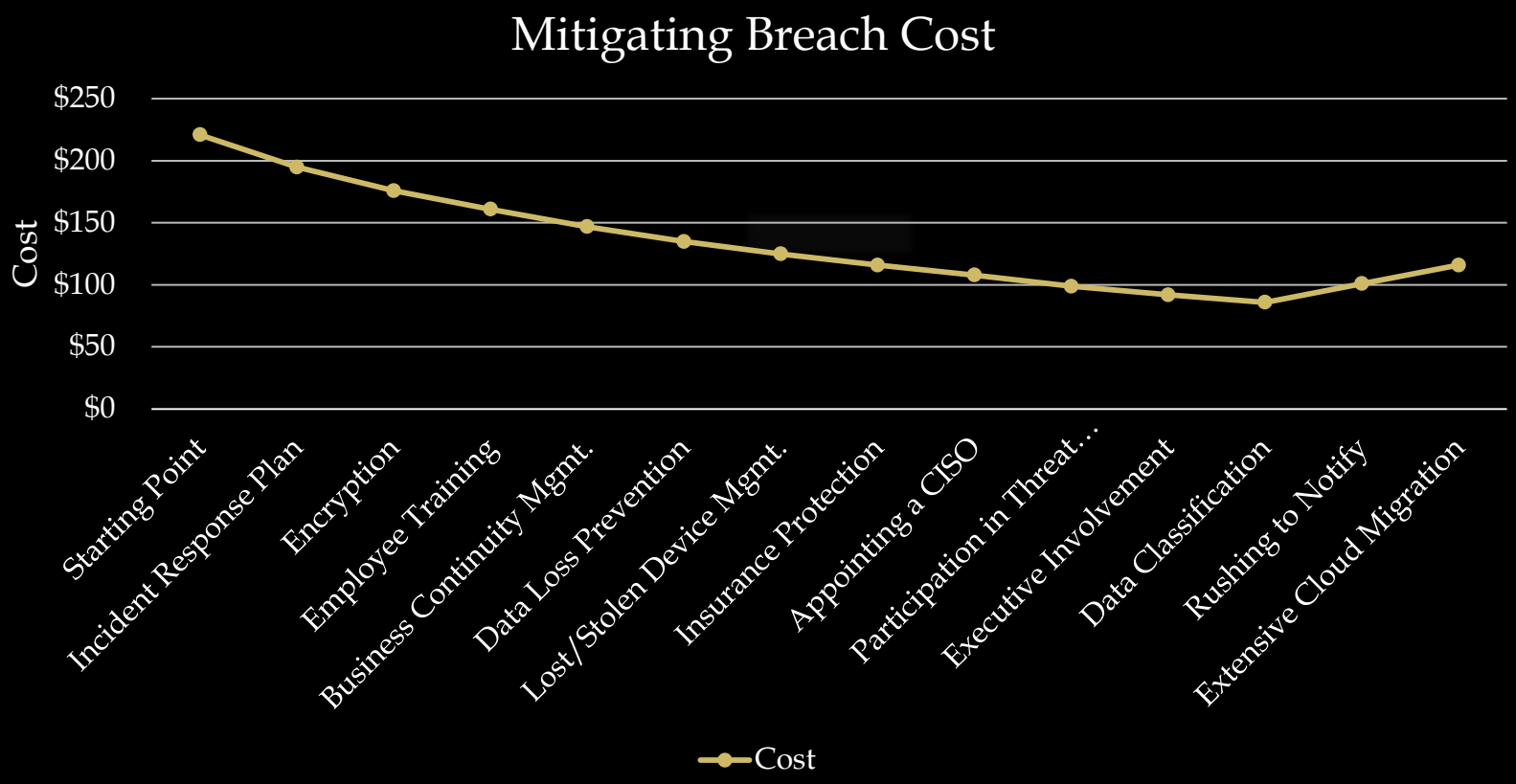
By ANDREW E. KRAMER
SEPTEMBER 27, 2016

BIYSK, Russia — Living anonymously, down a winding road in the wilderness of western Siberia, not far from the Mongolian border, the only person so far

Speed Matters!

- **The longer it takes to detect, the more it costs.**
- **70% of attackers move from the initial victim to a secondary target within 24 hours.**
- **An attacker is in your environment for over 200 days before detection**
- **Victims MUST report incidents quickly!**

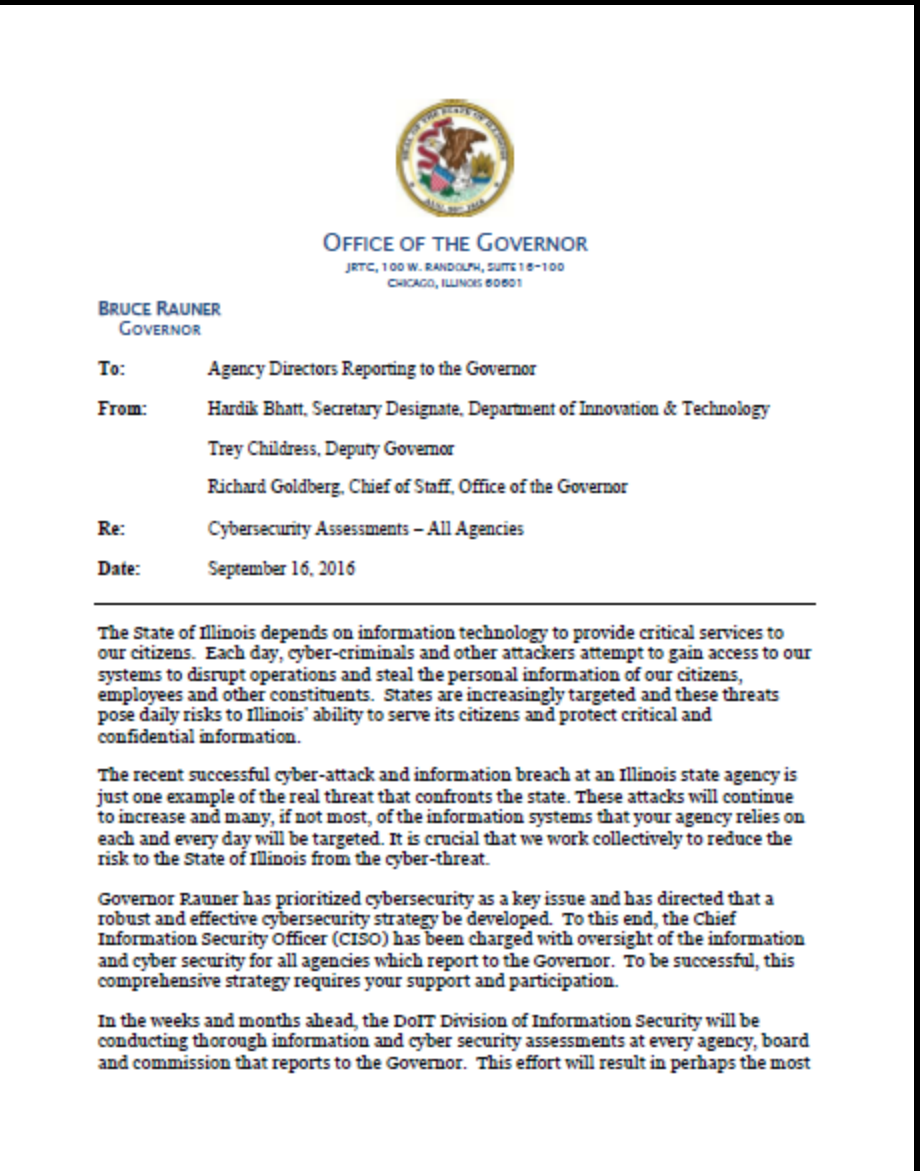
What Can Help?



How is it happening?

- **We DO know what we DO know! (known software vulnerabilities)**
- **Phishing is still the biggest sport (it's easy)**
- **63% of breaches involved weak, default or stolen passwords (we just don't get it – Multi-factor!)**
- **Social Unrest = Increased Attacks**
- **Web Applications have weaknesses (many easy to fix – just find them!)**
- **We all make mistakes. (human errors cost us)**

Letter to All Directors September 16, 2016



OFFICE OF THE GOVERNOR
JRTC, 100 W. RANDOLPH, SUITE 16-100
CHICAGO, ILLINOIS 60601

BRUCE RAUNER
GOVERNOR

To: Agency Directors Reporting to the Governor

From: Hardik Bhatt, Secretary Designate, Department of Innovation & Technology
Trey Childress, Deputy Governor
Richard Goldberg, Chief of Staff, Office of the Governor

Re: Cybersecurity Assessments – All Agencies

Date: September 16, 2016

The State of Illinois depends on information technology to provide critical services to our citizens. Each day, cyber-criminals and other attackers attempt to gain access to our systems to disrupt operations and steal the personal information of our citizens, employees and other constituents. States are increasingly targeted and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information.

The recent successful cyber-attack and information breach at an Illinois state agency is just one example of the real threat that confronts the state. These attacks will continue to increase and many, if not most, of the information systems that your agency relies on each and every day will be targeted. It is crucial that we work collectively to reduce the risk to the State of Illinois from the cyber-threat.

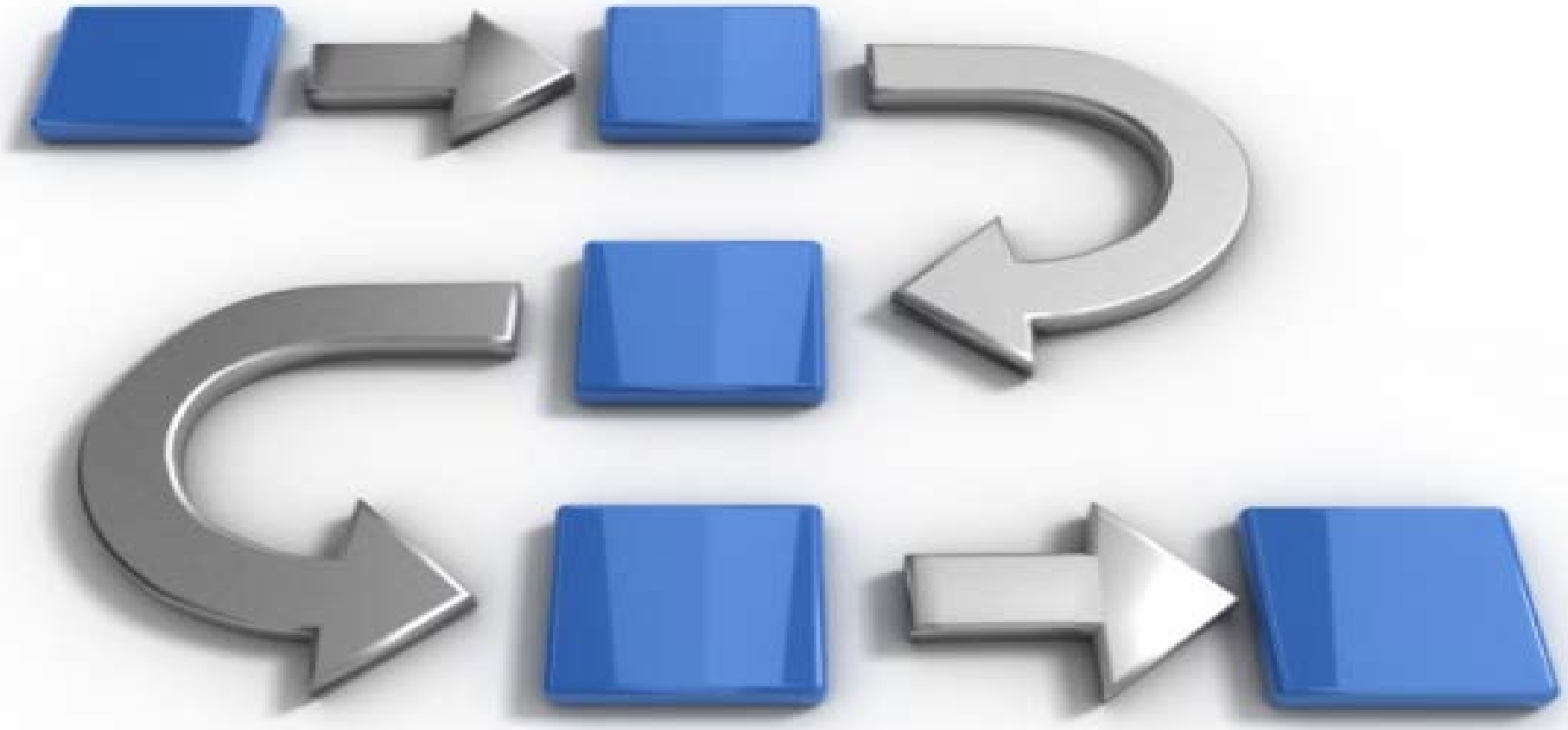
Governor Rauner has prioritized cybersecurity as a key issue and has directed that a robust and effective cybersecurity strategy be developed. To this end, the Chief Information Security Officer (CISO) has been charged with oversight of the information and cyber security for all agencies which report to the Governor. To be successful, this comprehensive strategy requires your support and participation.

In the weeks and months ahead, the DoIT Division of Information Security will be conducting thorough information and cyber security assessments at every agency, board and commission that reports to the Governor. This effort will result in perhaps the most

- Governor Rauner has prioritized cybersecurity as a priority issue
- Spoke of the ongoing cyber threat that faces the State
- Referenced recent breach at a State of Illinois agency
- Has charged DoIT with oversight and direction of cybersecurity matters for all agencies under the Governor
- Requested support from the Directors in completing comprehensive cybersecurity assessments across all agencies

Information Security Assessments

THE PROCESS



Information Security Assessments

Assessment Planning

- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Information Security Assessments

Assessment Planning

- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery

- Information Gathering
- Policy Review
- Security Roles Identification

Information Security Assessments

Assessment Planning

- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery

- Information Gathering
- Policy Review
- Security Roles Identification

Vulnerability Scanning

- Address High Risks Immediately
- Remediation Plans
- Risk Acceptance – Directors
- Commence Initial Monitoring

Information Security Assessments

Assessment Planning

- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery

- Information Gathering
- Policy Review
- Security Roles Identification

Vulnerability Scanning

- Address High Risks Immediately
- Remediation Plans
- Risk Acceptance – Directors
- Commence Initial Monitoring

Risk Assessment

- ID/Verify Applications and Data
- Identify Cloud Usage
- Security Controls Review
- Risk Rating

Information Security Assessments

Assessment Planning

- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery

- Information Gathering
- Policy Review
- Security Roles Identification

Vulnerability Scanning

- Address High Risks Immediately
- Remediation Plans
- Risk Acceptance – Directors
- Commence Initial Monitoring

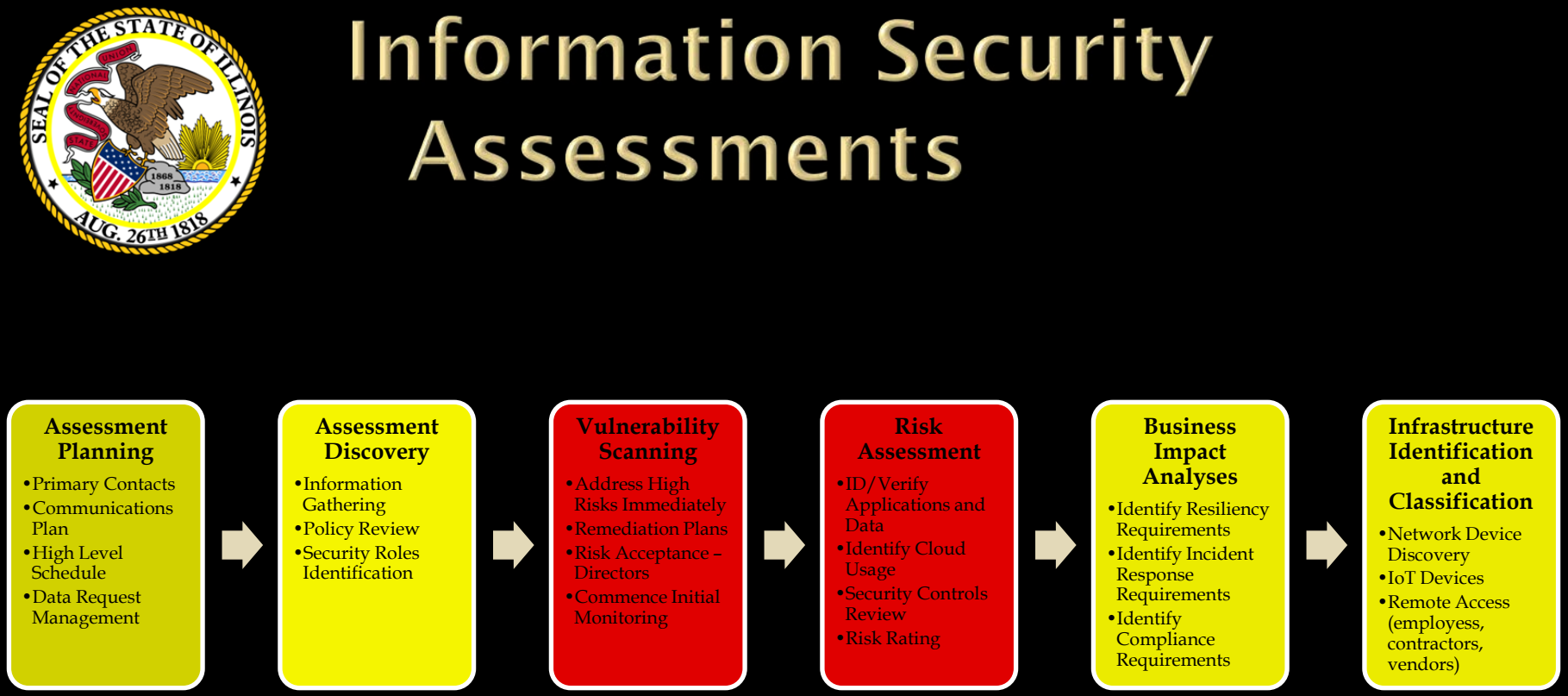
Risk Assessment

- ID/Verify Applications and Data
- Identify Cloud Usage
- Security Controls Review
- Risk Rating

Business Impact Analyses

- Identify Resiliency Requirements
- Identify Incident Response Requirements
- Identify Compliance Requirements

Information Security Assessments



Information Security Assessments

Information Security Assessments

Reduced Vulnerabilities

Information Security Assessments

Reduced Vulnerabilities

Assessment Planning
- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery
- Information Gathering
- Policy Review
- Security Roles Identification

Vulnerability Scanning
- Address High Risks Immediately
- Remediation Plans
- Risk Acceptance – Directors
- Commence Initial Monitoring

Risk Assessment
- ID/Verify Applications and Data
- Identify Cloud Usage
- Security Controls Review
- Risk Rating

Business Impact Analyses
- Identify Resiliency Requirements
- Identify Incident Response Requirements
- Identify Compliance Requirements

Infrastructure Identification and Classification
- Network Device Discovery
- IoT Devices
- Remote Access (employess, contractors, vendors)

Critical Data Protection
- Identify Data Sharing Agreements
- Classify Data
- Apply Security Protections
- Establish Data Monitoring

Better Security Controls

Information Security Assessments

Reduced Vulnerabilities

Reduced Risk

Assessment Planning
- Primary Contacts
- Communications Plan
- High Level Schedule
- Data Request Management

Assessment Discovery
- Information Gathering
- Policy Review
- Security Roles Identification

Vulnerability Scanning
- Address High Risks Immediately
- Remediation Plans
- Risk Acceptance – Directors
- Commence Initial Monitoring

Risk Assessment
- ID/Verify Applications and Data
- Identify Cloud Usage
- Security Controls Review
- Risk Rating

Business Impact Analyses
- Identify Resiliency Requirements
- Identify Incident Response Requirements
- Identify Compliance Requirements

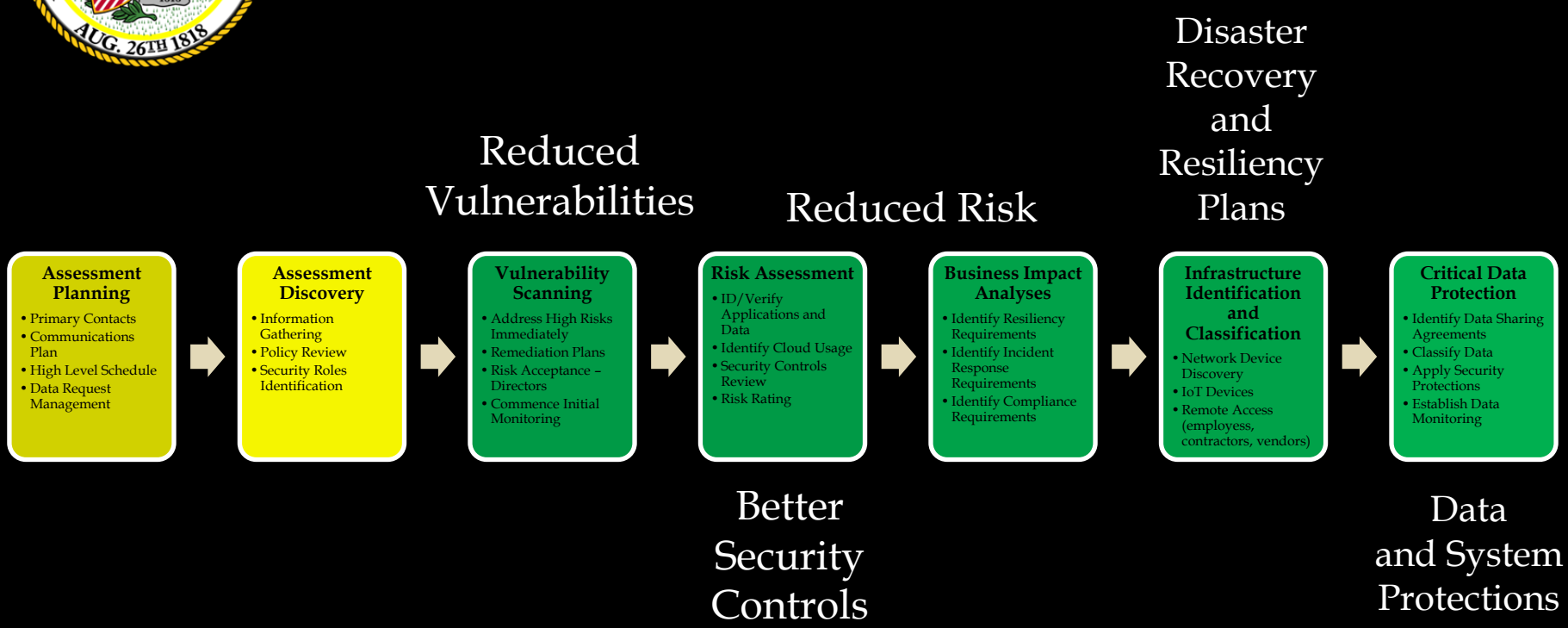
Infrastructure Identification and Classification
- Network Device Discovery
- IoT Devices
- Remote Access (employess, contractors, vendors)

Critical Data Protection
- Identify Data Sharing Agreements
- Classify Data
- Apply Security Protections
- Establish Data Monitoring

Better Security Controls

Information Security Assessments

Information Security Assessments



Information Security Assessments

Risk Assessment

- ID/Verify Applications and Data
- Identify Cloud Usage
- **Security Controls Review**
- Risk Rating

Vision Statement - A secure and resilient cybersecurity environment which facilitates and protects the business of the state of Illinois, reduces risk and protects privacy, while promoting innovation, economic growth and transparency.

State of Cybersecurity in 2015

Top Characteristics of the Initial State

- Lack of measurable outcomes as applicable to cyber security which display value to stakeholders.
- Inconsistent executive support regarding the prioritization of cyber security. Lack of specific authority and processes to direct resources to address critical security controls at state agencies. Competing priorities between security and business resources. Lack of wide understanding of the criticality of enterprise information security.
- Lack of a comprehensive security awareness program.
- Cybersecurity efforts and teams are decentralized and lack common standards and direction.
- Lack of uniformity on how security standards are applied. Lack of implementation of critical security controls and lack of consistent inventory practices for cyber-assets across state agencies.
- Inconsistent practices and expertise across entities in identifying that an attack or incident is taking place or has taken place.
- Cyber-risk information is not consistently shared across the state as an enterprise.
- Lack of a statewide cyber response plan as part of the Illinois Emergency Response Plan
- Absence of consistent risk management practices across state agencies. Security risks are either not known or not addressed.
- Lack of standardized cybersecurity policies across the state.
- Lack of sufficient cybersecurity expertise.

Key Initiatives

Cybersecurity awareness training for all state employees

Campaign to involve the Governor's Cabinet in cybersecurity oversight

Cybersecurity Strategic Plan which identifies funding and staffing needs.

Cybersecurity Governance and Authority structure for the state of Illinois

Strategy for the adoption of a common cybersecurity framework

Proactive threat detection training and technology sharing and innovation

Cybersecurity information sharing initiative (builds on STIC, MS-ISAC, FBI)

Cyber Disruption Strategy integrated into the State Emergency Operations Plan

Risk Management framework guidelines, policies and training for all state agencies

Model cybersecurity policies deployment across all state agencies

Illinois Cybersecurity Workforce Development Plan

Top Underlying Beliefs and Assumptions

Efforts to improve cybersecurity must properly reflect the borderless, interconnected, and global nature of today's cyber environment.

Efforts to improve cybersecurity must be based on risk management.

Efforts to improve cybersecurity must focus on awareness.

Cybersecurity efforts must be able to adapt rapidly to emerging threats, technologies, and business models.

Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.

Efforts to improve cybersecurity must more directly focus on bad actors and their threats.

Sufficient funding and resources will be provided to further the overall strategy.

All agencies will participate toward the success of the cybersecurity strategy.

State of Cybersecurity in 2016

Top Characteristics of the End State

- Illinois' cybersecurity strategies and programs are continually aligned with the business strategies of Illinois agencies, boards and commissions as well as the enterprise as whole.
- Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies.
- A culture of cyber-risk awareness at all levels of state government has been created and is continually enhanced.
- Illinois utilizes a common framework for cybersecurity across all state agencies.
- Illinois has developed and maintains a proactive approach to threat and attack detection and rapidly and effectively responds to mitigate the threats and reduce the impact to the state.
- Cybersecurity planning is prevalent during all phases of the solution development
- Emerging information security threats and vulnerabilities are appropriately shared across Illinois agencies, boards and commissions in a reliable and timely manner.
- Illinois' response to a significant cyber disruption is fully defined, exercised and effective. Cyber response is governed by the Cybersecurity Response Annex in the Illinois Emergency Operations Plan.
- Effective and consistent cybersecurity policies are in place across all state agencies.
- Illinois' cybersecurity workforce is well-trained and continually developed.

Statement of Risk - The lack of a comprehensive and consistent approach to cybersecurity strategy across the state poses an immediate threat to the State of Illinois and places the confidentiality, integrity and availability of critical information in jeopardy and poses risks to privacy assurances our citizens expect and deserve.

Vision Statement - A secure and resilient cybersecurity environment which facilitates and protects the business of the state of Illinois, reduces risk and protects privacy, while promoting innovation, economic growth and transparency.

State of Cybersecurity in 2015

Top Characteristics of the Initial State

- Lack of measurable outcomes as applicable to cyber security which display value to stakeholders.
- Inconsistent executive support regarding the prioritization of cyber security. Lack of specific authority and processes to direct resources to address critical security controls at state agencies. Competing priorities between security and business resources. Lack of wide understanding of the criticality of enterprise information security.
- Lack of a comprehensive security awareness program.
- Cybersec… and lack …
- Lack of u… applied. L… controls a… cyber-ass…
- Inconsiste… identifying… has taken place.
- Cyber-risk information is not consistently shared across the state as an enterprise.
- Lack of a statewide cyber response plan as part of the Illinois Emergency Response Plan
- Absence of consistent risk management practices across state agencies. Security risks are either not known or not addressed.
- Lack of standardized cybersecurity policies across the state.
- Lack of sufficient cybersecurity expertise.

Key Initiatives

Cybersecurity awareness training for all state employees

Campaign to involve the Governor's Cabinet in cybersecurity oversight

Cybersecurity Strategic Plan which identifies funding and staffing needs.

Cybersecurity Governance and Authority structure for the state of Illinois

Strategy for the adoption of a common cybersecurity framework

Proactive threat detection training and technology sharing and innovation

Cybersecurity information sharing initiative (builds on STIC, MS-ISAC, FBI)

Cyber Disruption Strategy integrated into the State Emergency Operations Plan

- Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies.

Efforts to improve cybersecurity must be based on risk management.

Efforts to improve cybersecurity must focus on awareness.

Cybersecurity efforts must be able to adapt rapidly to emerging threats, technologies, and business models.

Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.

Efforts to improve cybersecurity must more directly focus on bad actors and their threats.

Sufficient funding and resources will be provided to further the overall strategy.

All agencies will participate toward the success of the cybersecurity strategy.

State of Cybersecurity in 2016

Top Characteristics of the End State

- Illinois' cybersecurity strategies and programs are continually aligned with the business strategies of Illinois agencies, boards and commissions as well as the enterprise as whole.
- Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies.
- A culture of cyber-risk awareness at all levels of state government has been created and is continually enhanced.
- Illinois utilizes a common framework for …les.
- …s a proactive …tion and …nitigate the … state.
- …during all …
- Emerging information security threats and vulnerabilities are appropriately shared across Illinois agencies, boards and commissions in a reliable and timely manner.
- Illinois' response to a significant cyber disruption is fully defined, exercised and effective. Cyber response is governed by the Cybersecurity Response Annex in the Illinois Emergency Operations Plan.
- Effective and consistent cybersecurity policies are in place across all state agencies.
- Illinois' cybersecurity workforce is well-trained and continually developed.

Statement of Risk - The lack of a comprehensive and consistent approach to cybersecurity strategy across the state poses an immediate threat to the State of Illinois and places the confidentiality, integrity and availability of critical information in jeopardy and poses risks to privacy assurances our citizens expect and deserve.

Illinois Department of Innovation & Technology - Risk Assessment Framework

Objectives

- Improved standardization across agencies, clusters, committees, and departments
- More robust and resilient risk management practices

Core domains

- Governance Organization
- Data Privacy & Protection
- Asset Management
- Security Operations
- IT Risk Strategy
- Vulnerability Management
- Identity Access Management
- Training & Awareness
- IT Risk Assessment
- Monitoring, Communication & Reporting

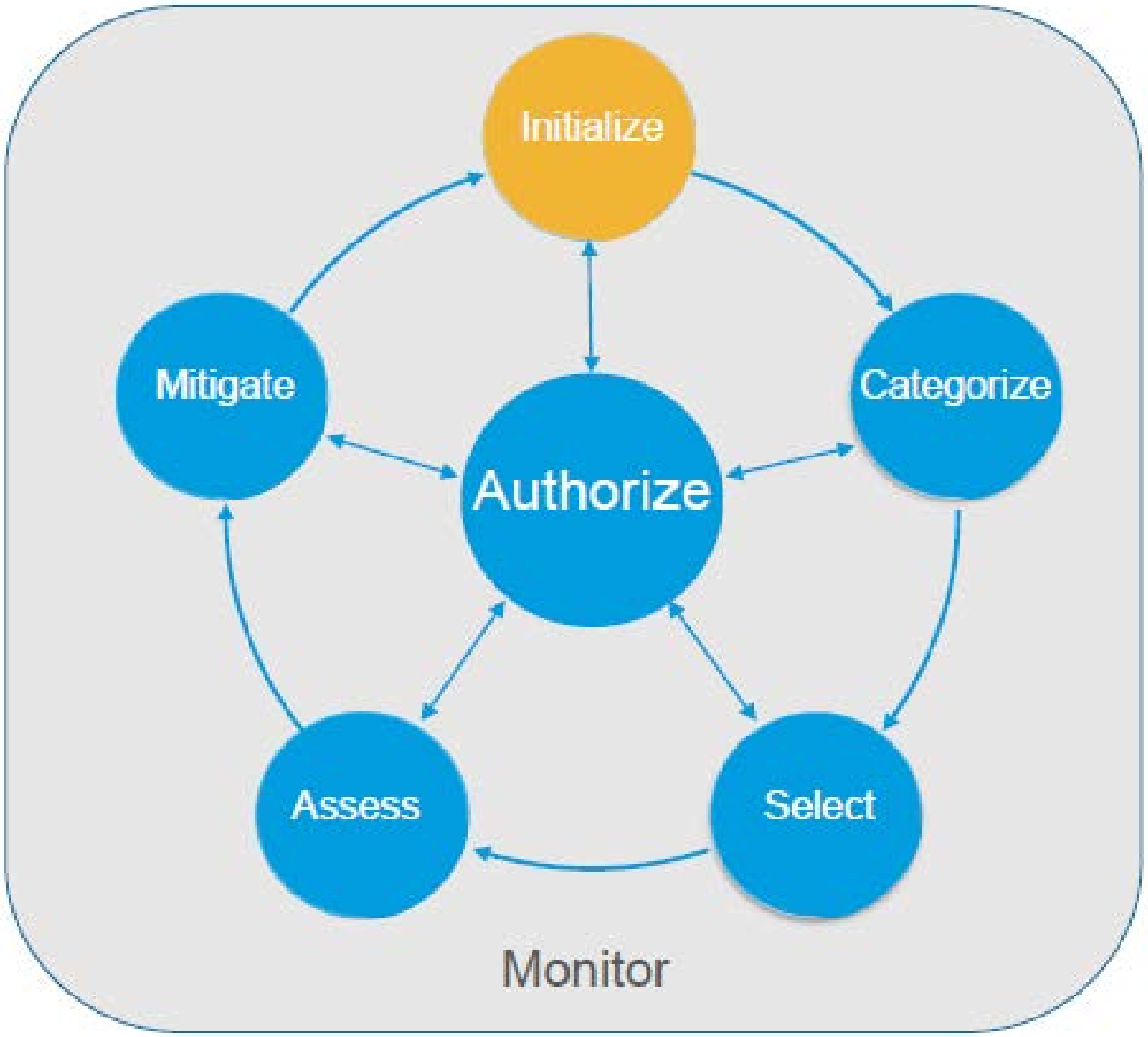
Operating model components

1. **Governance & Oversight**
   The organizational structure, committees, policies, roles and responsibilities for IT risk management
2. **Management Processes & Control Activities**
   Processes and controls to manage IT risks across the organization
3. **Culture & People**
   Appropriate training and awareness to promote an understanding and further the objectives of the IT risk management program
4. **Monitoring, Communication & Reporting**
   Ongoing monitoring, communication and reporting of risk and performance of controls across the organization

Illinois Department of Innovation & Technology
Risk Assessment Framework

- NIST-based model
- Includes robust Threat Analysis (TARA-based - Mitre)
- Lean implementation to make success more likely
- As automated as possible (Risk Management Workbook)
- Roles, Responsibilities and efforts aligned with the organization –Agencies/clusters

Illinois Department of Innovation & Technology
Risk Assessment Framework



Illinois Department of Innovation & Technology
Risk Assessment Framework

State of Illinois (Department of Innovation & Technology)
Information Security Organization Risk Assessment Framework: Self-Assessment Tool

Document Overview

This information security self-assessment tool provides an information security risk assessment framework for the State of Illinois (DoIT) by integrating control requirements and guidelines from National Institute of Standards and Technology (NIST) 800-53 Rev. 4.

Table of Contents

Version Control

Version	Updated by	Date modified	Change description
1.0		10/21/2016	Initial draft

Illinois Department of Innovation & Technology
Risk Assessment Framework

Information Security Component	Domains	Sub-Domains
Governance & Oversight	2	5
Management Processes & Controls	6	43
Culture & People	1	4
Monitoring, Communications and Reporting	1	5

75 Specific Risk Statements
(each with multiple guidelines)

Illinois Department of Innovation & Technology
Risk Assessment Framework

G.2	Security incidents are not managed with a consistent and effective approach.	Incident Response Plans are tested periodically. These tests are documented.	IR-3 The organization: 1. Tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.
G.2	Security incidents are not managed with a consistent and effective approach.	The organization has a robust Incident Response Program that includes contingencies and the adjustment of the plan based on experience.	IR-4 The organization: 1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; 2. Coordinates incident handling activities with contingency planning activities; and 3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
G.3	Lack of a Security Incident Response Program may result in improper identification and handling of security events.	Information security incidents are tracked and documented.	IR-5 The organization: 1. Tracks and documents information system security incidents.

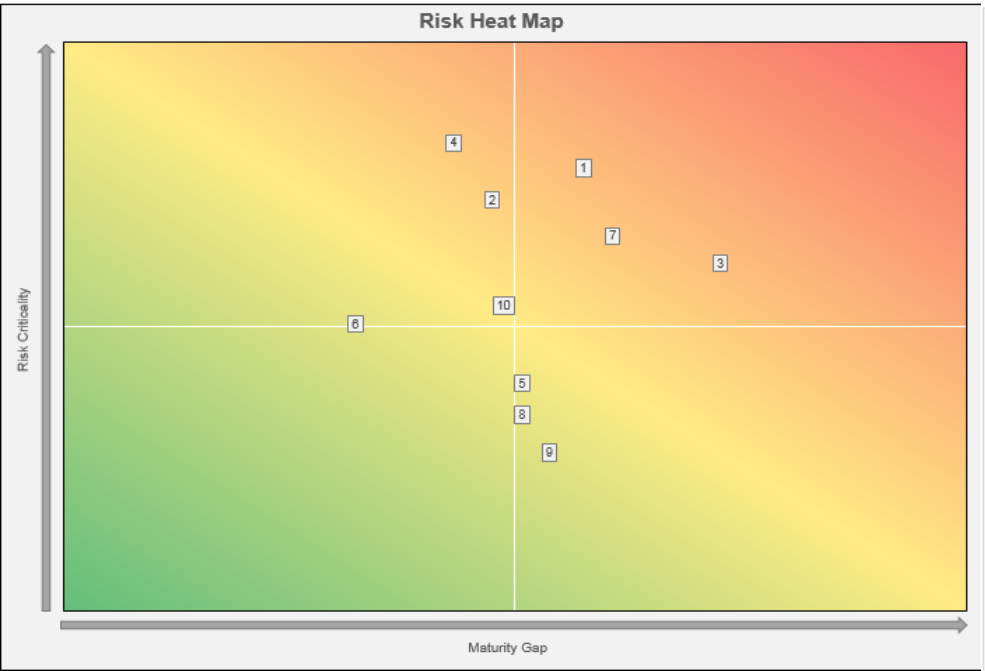
Illinois Department of Innovation & Technology
Risk Assessment Framework

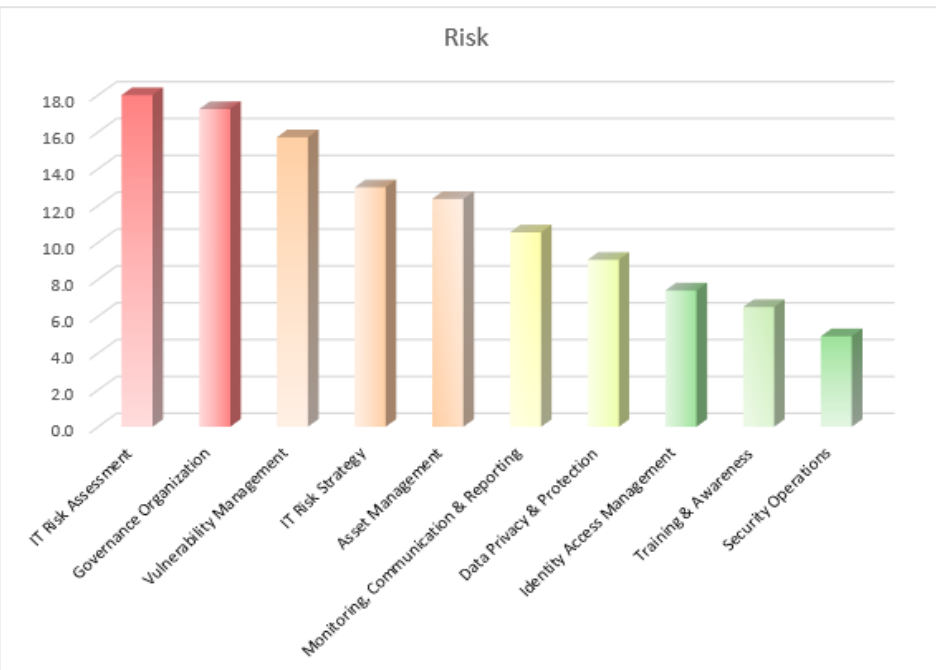
Score	Strength	Breadth	Rigor
1	Little to no protection	Little or no application across the organization	Ad-hoc process; not formally documented
2	No significant protection	Some application in selected areas across the organization	Repeatable process; not formally documented
3	Meaningful protection with little to no consistency in enforcement	Application in critical areas across the organization	Standard repeatable process; formally documented
4	Strong protection with consistent in enforcement	Application in most areas across the organization	Managed process with defined metrics driving toward control objectives
5	Maximum protection and consistent enforcement	Application in all possible areas across the organization	Optimized process; continuously improving; automated if possible

State of Illinois (DoIT)
Information Security organization Risk Assessment Framework: Self-Assessment Tool

Risk Dashboard

#	Domain	Maturity	Gap	Likelihood	Impact	Criticality	Risk
3	IT Risk Assessment	2.0	3.0	3.0	2.0	6.0	18.0
1	Governance Organization	2.7	2.3	2.8	2.8	7.5	17.3
7	Vulnerability Management	2.5	2.5	2.1	3.0	6.4	15.7
2	IT Risk Strategy	3.1	1.9	2.3	3.0	7.0	13.0
4	Asset Management	3.3	1.7	2.7	2.8	7.9	12.4
10	Monitoring, Communication & Reporting	3.1	1.9	2.0	2.7	5.3	10.6
5	Data Privacy & Protection	3.0	2.0	1.6	2.5	4.1	9.1
8	Identity Access Management	3.0	2.0	1.5	2.3	3.6	7.4
9	Training & Awareness	2.8	2.2	1.0	3.0	3.0	6.5
6	Security Operations	3.8	1.2	1.7	2.9	5.0	4.9

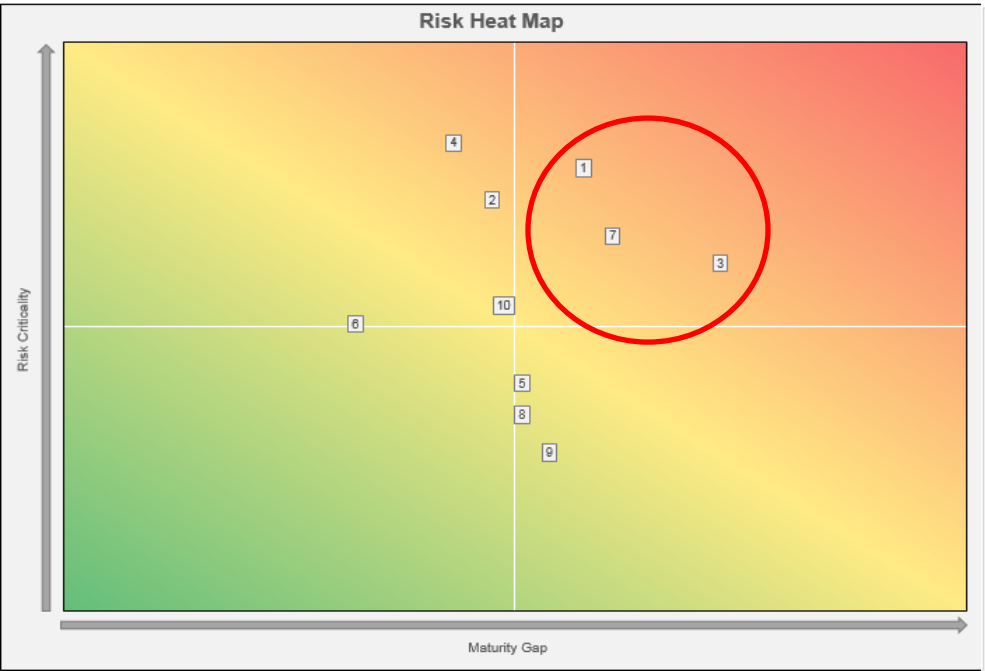


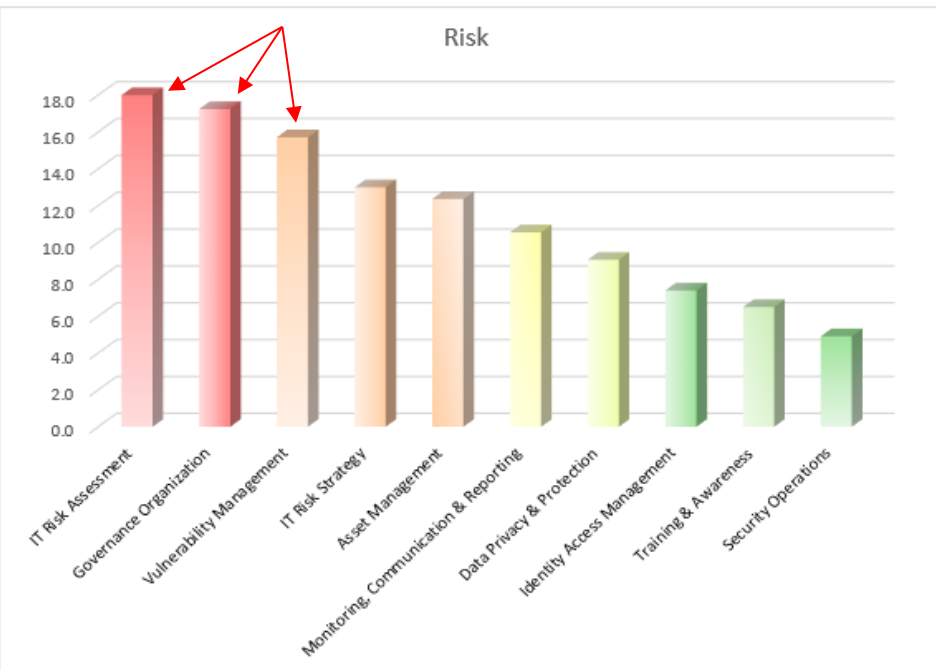


State of Illinois (DoIT)
Information Security organization Risk Assessment Framework: Self-Assessment Tool

Risk Dashboard

#	Domain	Maturity	Gap	Likelihood	Impact	Criticality	Risk
3	IT Risk Assessment	2.0	3.0	3.0	2.0	6.0	18.0
1	Governance Organization	2.7	2.3	2.8	2.8	7.5	17.3
7	Vulnerability Management	2.5	2.5	2.1	3.0	6.4	15.7
2	IT Risk Strategy	3.1	1.9	2.3	3.0	7.0	13.0
4	Asset Management	3.3	1.7	2.7	2.8	7.9	12.4
10	Monitoring, Communication & Reporting	3.1	1.9	2.0	2.7	5.3	10.6
5	Data Privacy & Protection	3.0	2.0	1.6	2.5	4.1	9.1
8	Identity Access Management	3.0	2.0	1.5	2.3	3.6	7.4
9	Training & Awareness	2.8	2.2	1.0	3.0	3.0	6.5
6	Security Operations	3.8	1.2	1.7	2.9	5.0	4.9





Illinois Department of Innovation & Technology
Risk Assessment Framework

IR-8 The organization:
Develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;

- Describes the structure and organization of the incident response capability;

- Provides a high-level approach for how the incident response capability fits into the overall organization;

- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

- Defines reportable incidents;

- Provides metrics for measuring the incident response capability within the organization;

- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

- Is reviewed and approved by the appropriate authority;

Vision Statement - A secure and resilient cybersecurity environment which facilitates and protects the business of the state of Illinois, reduces risk and protects privacy, while promoting innovation, economic growth and transparency.

State of Cybersecurity in 2015

Top Characteristics of the Initial State

- Lack of measurable outcomes as applicable to cyber security which display value to stakeholders.
- Inconsistent executive support regarding the prioritization of cyber security. Lack of specific authority and processes to direct resources to address critical security controls at state agencies. Competing priorities between security and business resources. Lack of wide understanding of the criticality of enterprise information security.
- Lack of a comprehensive security awareness program.
- Cybersecurity efforts and teams are decentralized and lack common standards and direction.
- Lack of uniformity on how security standards are applied. Lack of imple controls and lack of c cyber-assets across s
- Inconsistent practices identifying that an atta has taken place.
- Cyber-risk information across the state as ar
- Lack of a statewide cy the Illinois Emergency
- Absence of consistent risk management practices across state agencies. Security risks are either not known or not addressed.
- Lack of standardized cybersecurity policies across the state.
- Lack of sufficient cybersecurity expertise.

Key Initiatives

Cybersecurity awareness training for all state employees

Campaign to involve the Governor's Cabinet in cybersecurity oversight

Cybersecurity Strategic Plan which identifies funding and staffing needs.

Cybersecurity Governance and Authority structure for the state of Illinois

Strategy for the adoption of a common cybersecurity framework

Proactive threat detection training and technology sharing and innovation

Cybersecurity information sharing initiative (builds on STIC, MS-ISAC, FBI)

Cyber Disruption Strategy integrated into the State Emergency Operations Plan

Risk Management framework guidelines, policies and training for all state agencies

Model cybersecurity policies deployment across all state agencies

- A culture of cyber-risk awareness at all levels of state government has been created and is continually enhanced.
- Illinois utilizes a common framework for cybersecurity across all state agencies.

Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.

Efforts to improve cybersecurity must more directly focus on bad actors and their threats.

Sufficient funding and resources will be provided to further the overall strategy.

All agencies will participate toward the success of the cybersecurity strategy.

State of Cybersecurity in 2016

Top Characteristics of the End State

- Illinois' cybersecurity strategies and programs are continually aligned with the business strategies of Illinois agencies, boards and commissions as well as the enterprise as whole.
- Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies
- A culture of cyber-risk awareness at all levels of state government has been created and is continually enhanced.
- Illinois utilizes a common framework for cybersecurity across all state agencies.
- Illinois has developed and maintains a proactive approach to threat and attack detection and rapidly and effectively responds to mitigate the threats and reduce the impact to the state.
- Cybersecurity planning is prevalent during all phases of the solution development
- Emerging information security threats and vulnerabilities are appropriately shared across Illinois agencies, boards and commissions in a reliable and timely manner.
- Illinois' response to a significant cyber disruption is fully defined, exercised and effective. Cyber response is governed by the Cybersecurity Response Annex in the Illinois Emergency Operations Plan.
- Effective and consistent cybersecurity policies are in place across all state agencies.
- Illinois' cybersecurity workforce is well-trained and continually developed.

Statement of Risk - The lack of a comprehensive and consistent approach to cybersecurity strategy across the state poses an immediate threat to the State of Illinois and places the confidentiality, integrity and availability of critical information in jeopardy and poses risks to privacy assurances our citizens expect and deserve.

How can you help?


SEAL OF THE STATE OF ILLINOIS
UNION
NATIONAL
SOVEREIGNTY
STATE
1868
1818
AUG. 26TH 1818

Thank you!