Kansas Cybersecurity Transformation Plan

January 30, 2018

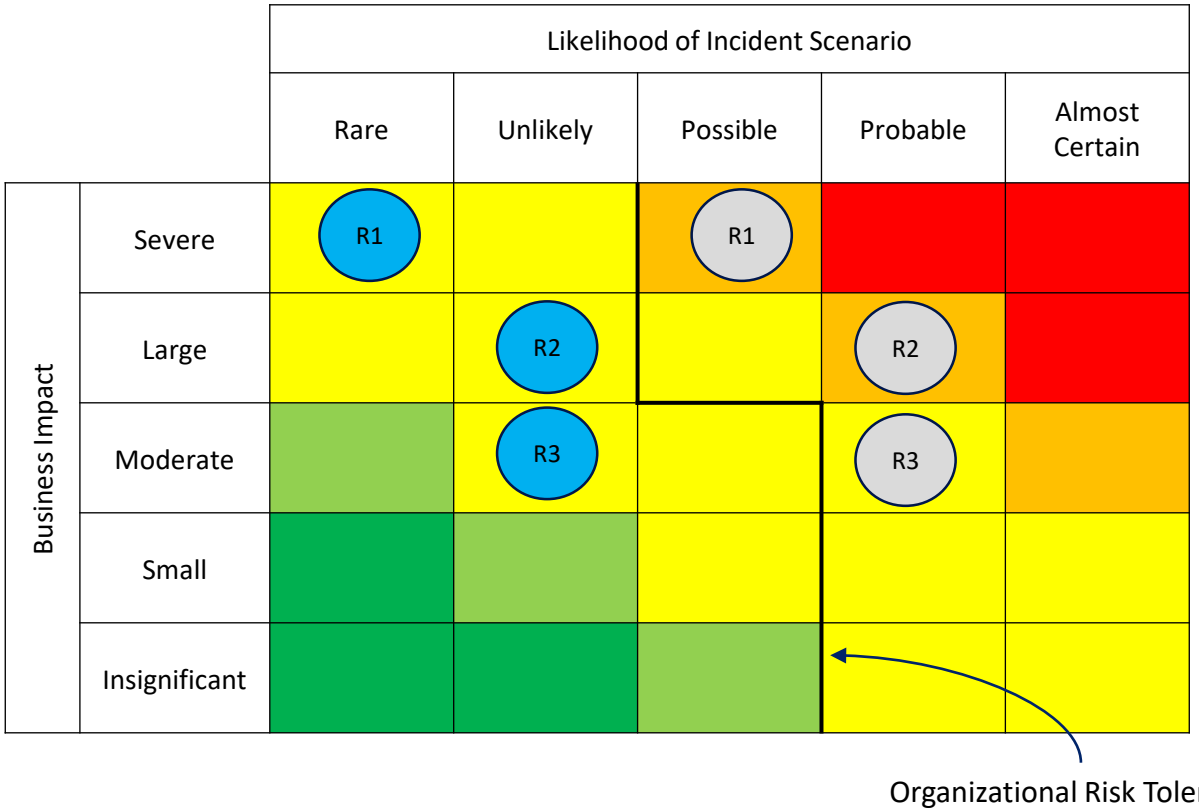
Securing the Data of our Citizens

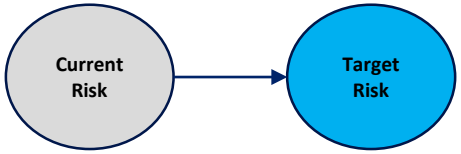
- Confidentiality
- Integrity
- Availability

Kansas

Cybersecurity Transformation Plan

Why





R1	Inability to provide services due to cyber attack or cyber terrorism
R2	Loss of citizen confidence due to sensitive information disclosure
R3	Financial liability due to data breach of sensitive information

Cybersecurity Transformation Plan
History

- **2010 Senate Bill 572**
  - Commissioned an Information Technology Consolidation Feasibility Study.
  - Study called for Consolidation of Security
- **2013 Security Survey Conducted**
  - The enterprise security office (at the time a two person office within OITS) conducted a survey to benchmark information security
  - The benchmarks revealed an underdeveloped security program with significant shortcomings in resources across all categories
  - Repeated LPA security audit findings over many consecutive years support conclusions of deficient security programs based on the survey
- **2014 Security Strategy Developed**
  - The ESO developed a detailed strategic plan to identify and improve security programs across state government
  - Strategic plan was developed in collaboration with industry experts and partners, and also included the security leadership of Regents institutions
  - First attempt at legislation, unable to find a sponsor to champion a security transformation effort (security buried in IT)

Cybersecurity Transformation Plan
History

- **2015 Third Party Consultants**
  - Recommended Consolidation/Collaboration
  - Outsourcing of various services
  - 2nd attempt at legislation, unable to find a sponsor to champion a security transformation effort (security still buried in IT)
- **2016 – Alvarez & Marsal efficiency study and security legislation introduced**
  - Recommended a centralized approach to Cyber Security.
  - 3rd attempt at legislation, the sponsor of the bill was the Vision 2020 Committee; the bill passed unanimously in the House, but fell victim to a “gut and go” in the Senate
- **2017 – Legislation introduced**
  - 4th attempt; 2 cyber bills were introduced with the same language: 1 in the Senate (SB204 sponsored by Ways and Means) and 1 in the House (HB2331 sponsored by the Committee on Government, Technology and Security). The House bill had the most activity and it was here that it was merged with an IT consolidation bill. Though the consolidated bill passed the house, it is speculated that it failed due to the IT consolidation initiative.

Cybersecurity Transformation Plan

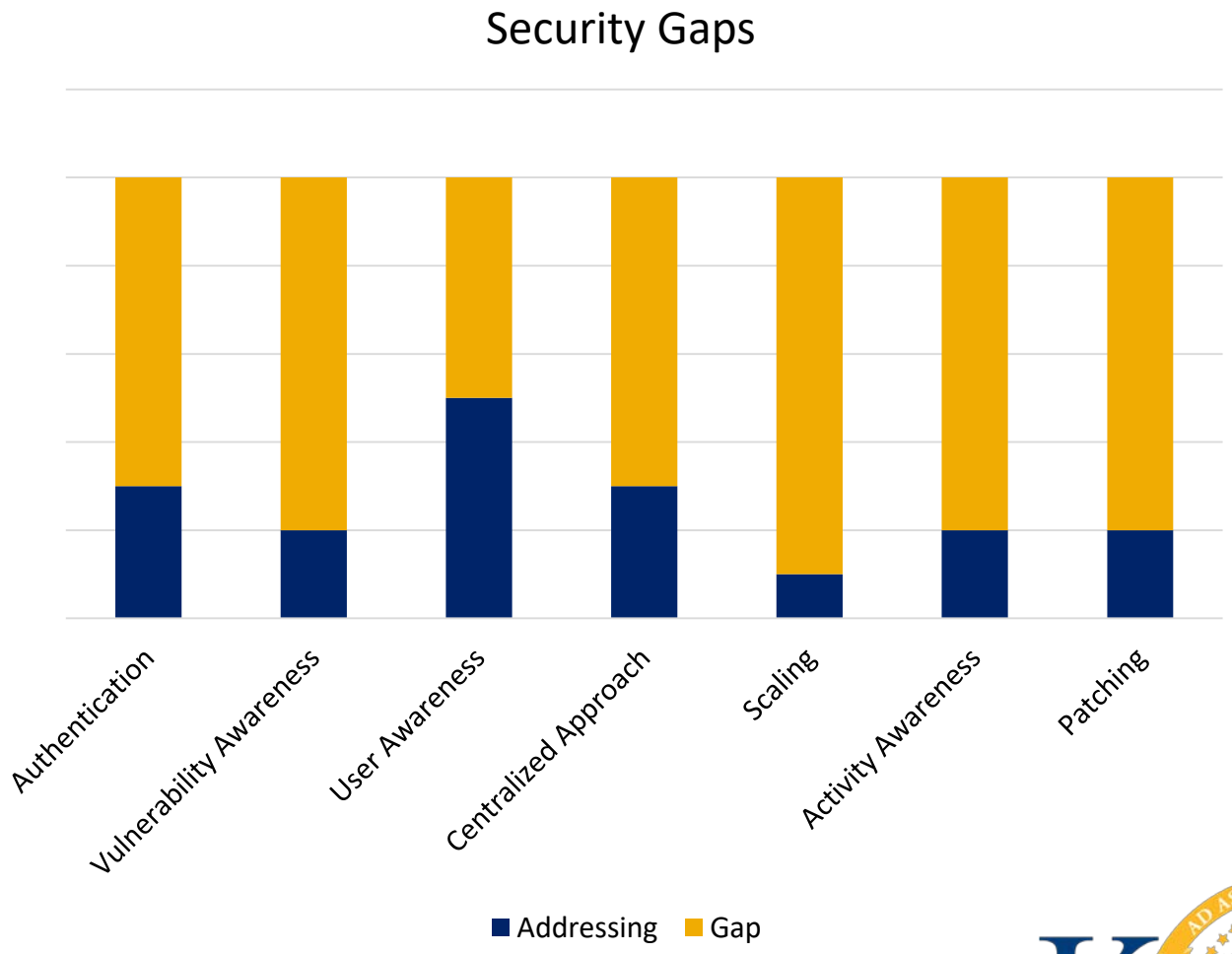
Why

Changes Required to move forward

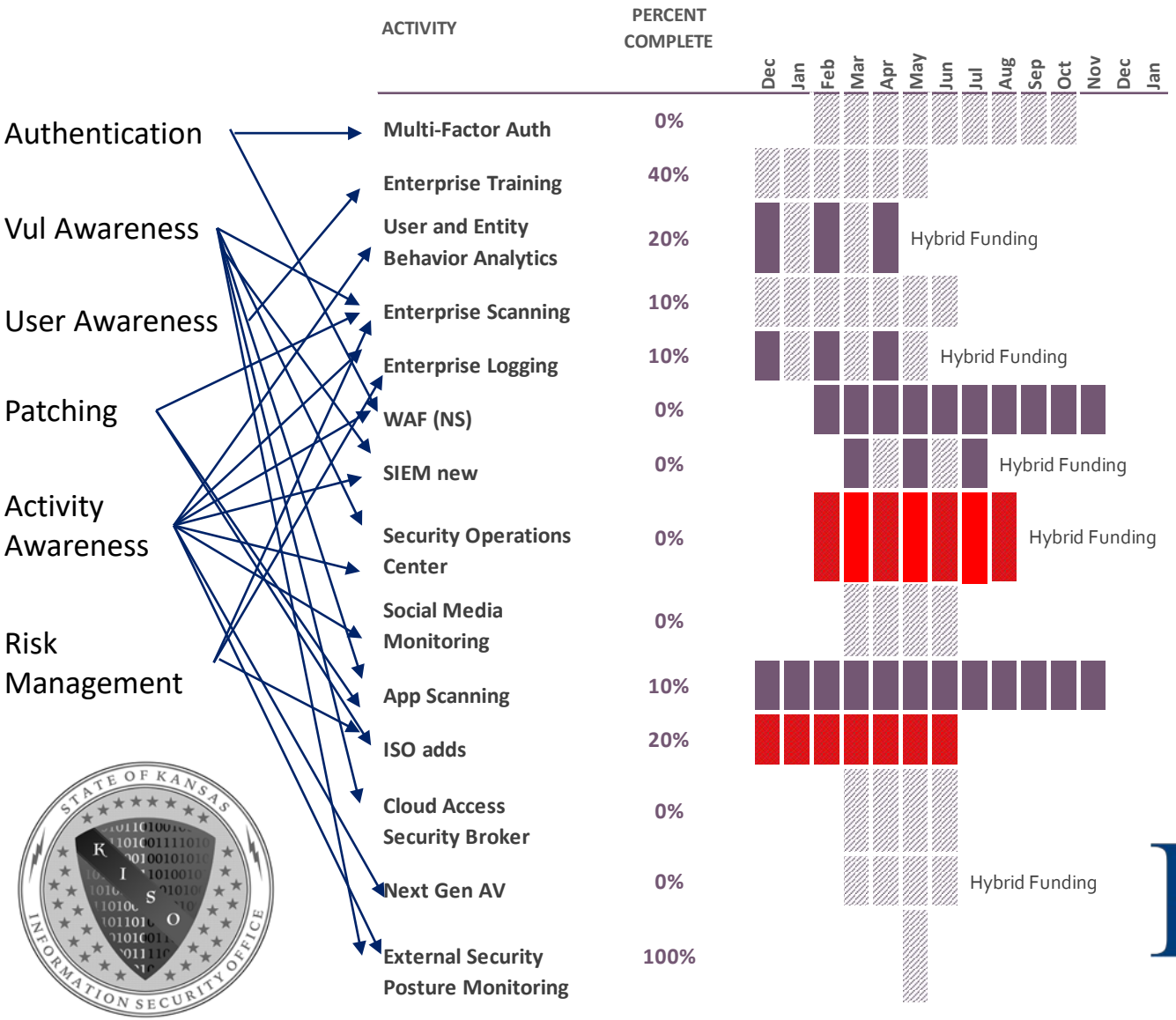
- Standardization across the Enterprise
- Economies of Scale
- Rapid Response
- Accountability
- Scalable
- Risk Mitigation
- Stable Funding

Cybersecurity Transformation Plan

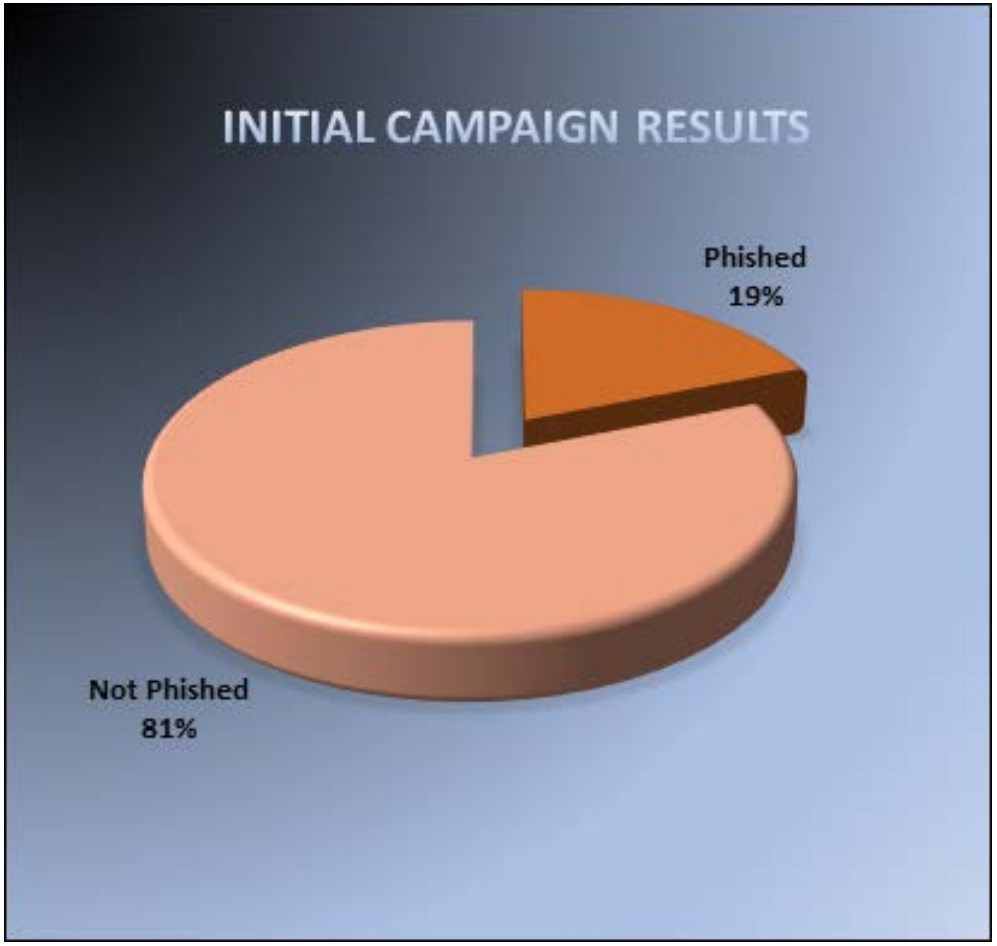
Why



Security Activities underway or needed



Phishing Campaign Conducted January



- 3600 State Employees were sent simulated Phishing Emails
- 19% (681) successfully phished
- 4% (139) submitted logon credentials
- If real, each successful phishing email could have led to malware installation
- Each user credential collected could have successfully compromised email accounts and possibly agency networks
- Baseline will be used to enhance the current security awareness training program

Kansas

Cybersecurity Transformation Plan

Vision and Guiding Principles

- **Vision Statement**

  A secure information network that facilitates the business of the State, protects privacy and reduces risk, all while promoting innovation, economic growth and transparency.

- **Strategic Guiding Principles**
  - Cybersecurity efforts must properly reflect the borderless, interconnected, and global nature of today's cyber environment
  - Cybersecurity efforts must be able to adapt rapidly to emerging threats, technologies, and business needs
  - Cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments
  - Cybersecurity efforts must be based on risk management
  - Cybersecurity efforts must maintain a focus on awareness
  - Cybersecurity must more directly focus on bad actors and their threats
  - Sufficient funding and resources must be provided to further the overall strategy

Cybersecurity Transformation Plan

Strategic Outcomes

- **Goal 1 – Protect State Information and Systems**
  - State information is protected from unauthorized disclosure
  - State information is trustworthy
  - State information and systems are available when needed
  - The State is capable of withstanding and quickly recovering from deliberate attacks, accidents or naturally occurring threats or incidents
- **Goal 2 – Reduce Cyber Risk**
  - 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 government has been created and is continually enhanced
  - Cybersecurity risk is clearly communicated understood, and owned by business executives
- **Goal 3 – Effective and Efficient Cybersecurity Capability**
  - State cybersecurity strategies and programs are continually aligned with the business strategies of State agencies, boards and commissions and the enterprise as whole
  - Cyber-risk is reduced through the deployment of information systems that are secure
  - The State rapidly identifies and disrupts cyber-attacks to minimize adverse impact on the State
  - Rapid, consistent and effective security incident response capabilities reducing impacts of security incidents, and response effectiveness is continually improved
  - The State's cybersecurity workforce is well-trained, continually developed and aligned with national standards

Cybersecurity Transformation Plan
Strategic Outcomes

- **Goal 4 – Enterprise Approach to Cybersecurity**
  - A centralized effective enterprise-wide information and cybersecurity program providing consistent cybersecurity protection across state agencies
  - The cybersecurity posture of the State continues to improve through the use of a common cybersecurity framework
  - Effective and consistent enterprise-wide cybersecurity policies are effectively communicated, monitored for compliance, resulting in a more secure enterprise
- **Goal 5 – A Cyber Secure State**
  - The State has established, exercised and continually improves an effective and inclusive cyber disruption strategy which will help reduce the impact of a cyber disruption on the State and its citizens
  - The State is leading efforts to improve the security of critical infrastructure and protect citizens from cybercrime
  - The State has developed and nurtured partnerships which foster continual learning and collaboration and effectively improves the State's cybersecurity posture.
  - The State contributes to the overall cybersecurity of the nation and utilizes national best practices and frameworks

Cybersecurity Transformation Plan

- **2018 – Legislation introduced (5th attempt)**
  - Establish the position of the Chief Information Security Officer (CISO); authorities; and responsibilities
    - Reports to the Governor
    - Annual reports to legislative committees
  - Establish the Kansas Information Security Office (KISO); authorities and responsibilities
    - Independent organization outside of IT
    - KISO resources assigned to agencies report to organizational leadership, not through IT
  - Establishes department head's responsibilities with regard to security
  - Establishes minimum security standards for all organizations connecting to the State network
  - Establishes minimum security standards for all State organizations that provide online or mobile services
  - Establishes requirement for background investigations for employees with access to sensitive information
  - Addresses sensitive data restrictions for KORA requests

Contact Information:

Joe Acosta
Chief Information Security Officer
Joe.Acosta@ks.gov
(785) 296-8434

Rod Blunt
Deputy Chief Information Security Officer
Rodney.Blunt@ks.gov
(785) 296-7440

Cybersecurity Transformation Plan

Organization Chart