Vision for Improving Performance in Texas State IT Projects: Measuring Quality & Cybersecurity

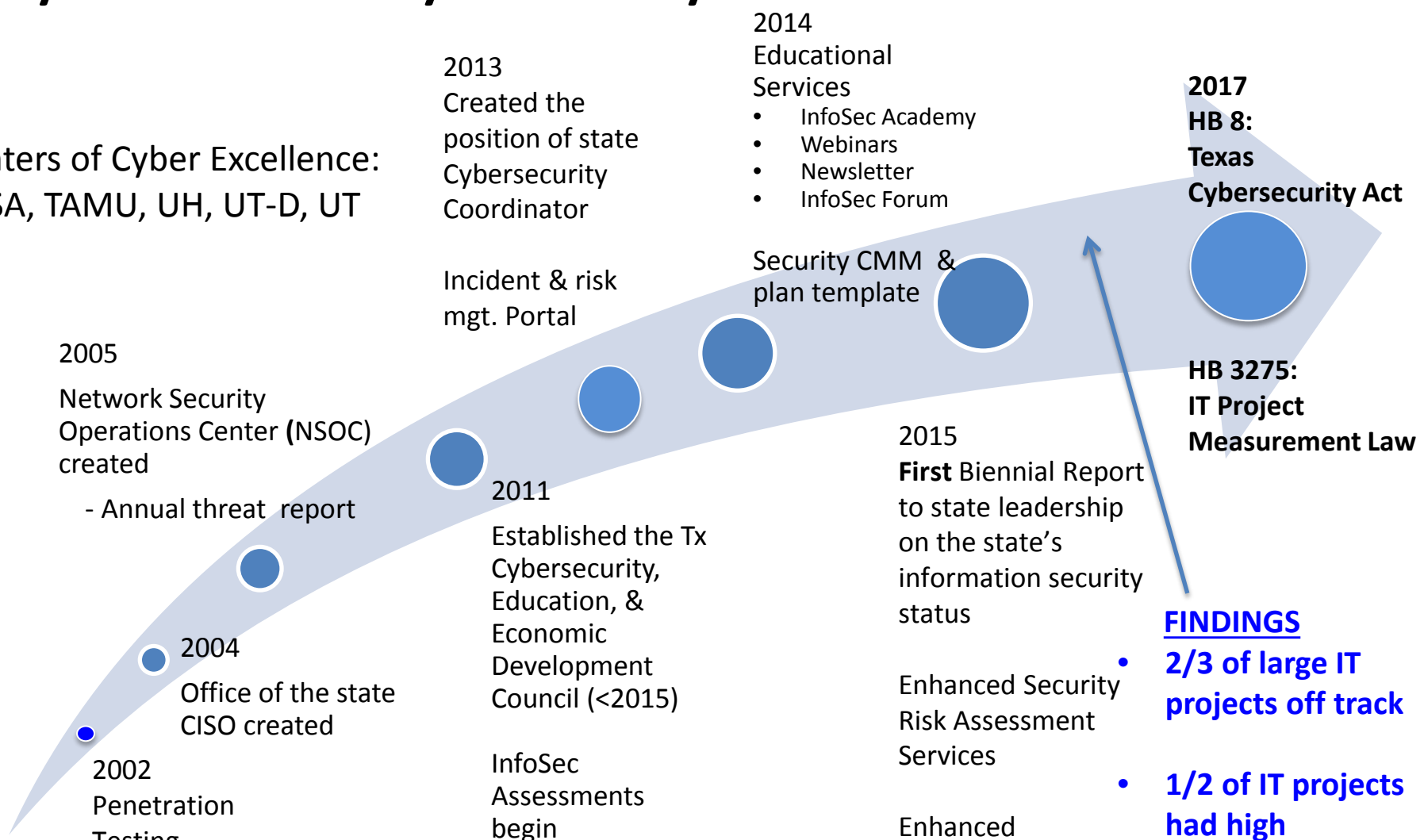
Presenter:
Marc Jones
Vice President, North American Public Sector
CAST Software

CISQ Volunteer

Prepared by:
Herb Krasner (in absentia)
Professor of Software Engineering, UT (Ret.)
CISQ Advisory Board Member
hkrasner@utexas.edu

Oct. 19, 2017

Cybersecurity History in Texas State Gov.



CHALLENGES

All recommendations, not required

100+ agencies - distributed & independent

FINDINGS

- **2/3 of large IT projects off track**
- **1/2 of IT projects had high cybersecurity & legacy failure risks**

Texas Cybersecurity Act: HB8 (9/1/17)

- Primary motivation: protect vital information assets; address vulnerabilities in aging IT infrastructure

Next steps: create/enhance these entities

IT staff reqts for cybersecurity training & certification	Tx State Cybersecurity Plan (coordinate with NIST, CERT, etc.)	Tx Agency Biennial Cybersecurity Assessment & Plan **required** **(+ exec. signing)**
Info. Sharing & Analysis Center (e.g. best practices)	Tx Cybersecurity Council (public & private) **required**	Tx Select Committees on Cybersecurity (House & Senate) (< 12/2017)
Required to report breaches ASAP to Agency & State CISO (emergency $$ if needed)	**Required** vulnerability and pen testing for selected systems	Election infrastructure cyber attack study

http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=85R&Bill=HB8

HB3275: Monitor Major[1] State Projects

- Collect data and report on performance indicators for: *schedule, cost, scope, and **quality***.
  - Indicators go out of bounds -> more intense scrutiny triggered, potentially requiring corrective action.
  - Indicators to be made visible via online, user-friendly dashboard; summarized annually in a report to state leaders.
  - Facilitates early warning of troubled projects
  - Helps establish baselines for improvement
  - http://www.legis.state.tx.us/BillLookup/Actions.aspx?LegSess=85R&Bill=HB3275
- Next step is policy/procedures/implementation:
  - http://it-cisq.org/measuring-it-project-performances-in-texas-house-bill-hb-3275-implications/
  - Monitoring **rules** created by Dec. 1st; law takes effect Jan. 1st
  - Definition of quality – in process
- Initial project execution capability assessment
  - To increase the likelihood of success, reduce risk, etc.

1. > $1M, and/or > 1 yr. or > 1 agency or …

Q&A

- Follow up questions?
  - *hkrasner@utexas.edu*
  - *marc.jones@it-cisq.org*

Cyber Resilience Measurement Concepts[1]

- Resilience is a family of related ideas, not a single thing. Its not just a technical system property.
  - The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources (MITRE, 2016)
    - System properties related to being able to withstand attacks and deviations from the intended state and go back to a pre-existing, or a desirable or acceptable, state.
    - Ability to deliver, maintain, improve IT services when facing cyber threats and related evolutionary changes
- Possible measures that characterize cyber resilience
  - *Dependability/availability* in the presence of flaws, faults, defects, vulnerabilities
  - *amount of disruption* that a system can tolerate under attack
  - *probability of correct service* given that an attack occurred
  - *set of probabilities* of the "levels of accomplishment" of a system's function under attack
- Cybersecurity Measurement (current data sources):
  - Risks –> default model
  - Threats (surface, vectors, scenarios, etc.)
  - Vulnerabilities (CVSS 3.0, Mitre CWE, CERT, **CISQ Security metric**)
  - Cyber security technical debt (definition TBD)
  - Using data from: antivirus and antispyware tools, intrusion detection systems, firewalls, patch management systems, security logs, vulnerability analyzers.

1. K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Ch. 1, L. Strigini,
DOI: 10.1007/978-3-642-29032-9_1,