Strategic Management of IT: The State Perspective

Kevin C. Desouza | kev.desouza@gmail.com
Gregory S. Dawson | gregorysdawson@gmail.com
Background

- Our Goal – To understand the drivers of strategic management of information technology in the public sector
  - Advancing the state of practice
- Team
  - Desouza and Dawson (co-Leads)
  - Rashmi Krishnamurthy (PhD student)
  - Kena Fedorschak (MBA student)
- Projects
  - IT Strategic Plans – Content Analysis
  - IT Metrics – Measuring the Value of IT
  - Alignment of IT Plans with State Objectives
  - IT Innovation, CIO Leadership, and Governance
How state governments are addressing cybersecurity

News about successful hacks of large companies seem to have become common place. In the recent Anthem cyber attack, hackers accessed the names, birth-dates, social security numbers, income, health status and many other details for companies’ customers. At present, Anthem does not even know the total number of records breached but estimates it to be “tens of millions”.

At present, government has been less affected by security breaches than the private sector. By late 2014, the Privacy Rights Clearinghouse (which maintains a list of all publicly reported data breaches) recorded 37 incidents involving government entities which included a data breach involving 800,000 employees and 2.9 million customers at the U.S. Postal Service, 950,000 job seekers in Oregon, and background data on 25,000 underground investigators at the U.S. Department of Homeland Security.

In speaking broadly about threats, General Vincent Stewart, Director of the Defense Intelligence Agency, commented that current intelligence gathering efforts afford a general
Cybersecurity

- Not a new issue
  - but it is increasing in prominence and impact
    - dependence on IT
    - distributed nature of IT ownership and control
    - disconnected (fragmented) security policies
    - humans, BYOD, social networks
    - transnational actors
- Cyberattacks originate locally and then scale globally
  - responsibility and accountability for security is distributed
  - uneven investment into security
Our Research

- Two goals
  - uncover if US states considered cybersecurity a strategic priority?
    - if yes, then what were they doing about it?
    - if no, why not and how can we raise awareness of the issue?
  - uncover access to cybersecurity information to state employees, citizens, and businesses
    - how can we increase information awareness on this critical issue?
Cybersecurity – IT Strategic Plans

- IT Strategic Plans
  - 35 States
    - not all states make their IT strategic plans readily accessible
- What did we find
  - wide disparity in how plans captured cybersecurity intentions, plans, and objectives
    - 4 Weak
    - 6 Aware
    - 14 Addressing
    - 11 Leaders
Cybersecurity – State Websites

- Websites a key information awareness platform
- What did we find
  - almost all States had a website dedicated to cybersecurity
  - content analysis of the websites revealed that
    - there are States that have fairly detailed IT security websites (e.g. Michigan)
    - a handful of States had documents and data on the website that were outdated (e.g. 2010 IT security plans with no recent updates)
    - some States have not update/refresh their main IT security page for several years
    - contact information and protocols of reporting cybersecurity concerns, issues, and incidents was difficult to find on 30% of the State IT security websites
Cybersecurity – State Websites

- Information on the websites could use a major overhaul
  - information on major types of cybersecurity attacks should be made more prominent
    - have clear definitions for each, reporting and response action steps
  - options for anonymous reporting of threats, risky and malicious behavior, and general feedback
  - contextualize and personalize information for employees
    - cloud computing → Dropbox
    - mobile security → Apps
  - update the website on a regular basis
    - do not simply link to news items on external sites
The Path Ahead

- Aligning cybersecurity with IT strategy
- Risks versus rewards for investments in IT security
- Mobile and cloud security
- Security across borders
Research Collaboration

- Opportunities to engage with us on research projects
- Contact –
  - Kevin C. Desouza
    - kev.desouza@gmail.com | http://www.kevindesouza.net