Government Business Council and CenturyLink
Issue Brief (Revised Version)
Survey Results
September 27, 2016

# Awareness & Analytics: Weapons of Choice in State & Local Cybersecurity

## Introduction

State and local governments increasingly find themselves pitted against a multitude of cyber threats unique to their regional and municipal oversight. Whereas the latest federal budget saw a 35 percent increase in cybersecurity spending over the previous year, the situation in state and local government remains comparatively more stagnant.[1] In 2016, for example, nearly two thirds of all state chief information security officers (CISOs) reported that their cybersecurity programs had received just 1 to 5 percent of their state's' overall IT budget.[2] Moreover, another 33 percent affirmed that their cybersecurity budget had made no gains from the previous year.[3] Consequently, state and local governments may feel they lack the centralized resources, strategy, and financial backing necessary to acquire and maintain a strong, agile cybersecurity workforce. This makes it all the more imperative for leaders in state and local government to maximize the resources they *do* have in order to weather the most damaging attacks from those seeking to steal sensitive information or access critical controls.

## A Priority Plagued By Difficulties

A GBC report released in August 2016 confirms cybersecurity's importance to state and local government leaders, with 77 percent believing their organization considers it a high priority when compared to other mission objectives. However, in spite of cybersecurity's recognized importance, state and local agencies continue to face a number of challenges when it comes to enhancing their cyber capabilities. Some of the more prominent hurdles are a lack of cyber awareness across government agencies, a shortage of cybersecurity personnel and talent, and ongoing budget constraints that make it difficult to invest in robust analytics packages. This may explain why a good portion of state and local agencies feel less confident regarding their cyber defenses, with 39 percent of respondents from this cohort reporting they feel more vulnerable to cyber threats than their federal counterparts.

A 2016 investigation by the State Auditor of California confirms these findings, identifying major vulnerabilities in the state's information controls.[4] Specifically, 73 out of the 77 state entities investigated had yet to achieve full compliance with the State's information security requirements, whether that be maintaining an inventory of information assets, consistently evaluating potential risks to such assets, or developing sound program management to address

---

[1] https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/fact_sheets/strengthening_federal_cybersecurity.pdf
[2] http://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf
[3] Ibid.
[4] https://www.bsa.ca.gov/pdfs/reports/2015-611.pdf

identified asset vulnerabilities. Considered a leader in cybersecurity, the findings on California are symptomatic of broader issues in state and local agencies across the country. In short, the perception that state and local agencies are particularly vulnerable isn't just suspicion; it's a fact, underscored by real pains that must be addressed swiftly and systematically before it is too late.

**Increasing Cyber Awareness Is Critical**

Among the vulnerabilities shared by state and local agencies, cyber awareness consistently emerges as a universal concern and top priority in the effort to improve network defenses. In fact, nearly 50 percent saw increased employee awareness as one of the leading priorities of the past year. This will likely remain the case, as 55 percent still believe that escalating such awareness efforts, in tandem with greater investment in cyber technologies, will enact the most positive effect on their agency's cybersecurity posture going forward.

However, if these awareness efforts are to be successful, agencies will need to ensure their employees receive comprehensive training in best practices and techniques. Currently, only 8 percent describe the training they've received as comprehensive, whether that entails instruction from subject matter professionals or enrolling in a cybersecurity course. Meanwhile, nearly half of respondents consider their training to be at a basic level, provided through department policy manuals or email instructions. Most concerning is that 1 in 5 claim to have not received any kind of cybersecurity awareness training whatsoever.

While Utah has experienced its share of cybersecurity problems in the past, including an infamous 2012 data breach that exposed the Social Security numbers and personal data of about 280,000 Medicaid recipients, the state recently drew praise for announcing its plans to enact a comprehensive cybersecurity awareness campaign.[5][6] Earlier this year, Utah's Division of Emergency Management (DEM) piloted a cybersecurity curriculum developed by Texas A&M Engineering Extension Service (TEEX).[7] The class takes students through a three day crash course in fundamental cybersecurity practices, with lessons on phishing scams and attack scenarios, plus live practice simulations that allow students to rehearse action plans in the incident of an attack.[8] Though more advanced than standard awareness programs for general employees, these specialized programs aim to bridge understanding between IT personnel and emergency operations on how to best respond *together* in the event of a cyber attack.

"What we've found across the U.S. is that the connection between the IT folks and the emergency operation center folks doesn't happen on a consistent basis," says Tony Crites, program director for preparedness programs at TEEX. "What we want to do is go out and say: 'Okay, folks, if it does happen, here are some of the resources that you have in your communities to effectively manage this type of event."[9]

---

[5] http://www.computerworld.com/article/2504542/security0/utah-cto-takes-fall-for-data-breach.html
[6] https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/
[7] http://www.routefifty.com/2016/02/teex-cybersecurity-incident-response/125790/?oref=rf-topic-river
[8] http://dem.utah.gov/2016/01/29/utah-dem-pilots-new-teex-cybersecurity-course/
[9] http://www.routefifty.com/2016/02/teex-cybersecurity-incident-response/125790/?oref=rf-topic-river

Like Utah, Colorado also recognizes that cybersecurity awareness isn't just an "IT thing." Rather, it's critical to operations in every department. That's why Colorado's CISO requires that at least 90 percent of all state employees receive cybersecurity awareness training while on the job.[10]

**Analytics As a Secret Weapon**

Many state and local agencies are also challenged by a lack of familiarity with robust analytics solutions. GBC's survey found that 55 percent of respondents are unaware if their organization even leverages analytics to improve threat detection. Equally concerning is that nearly 1 in 5 are certain their agency does not use and has no plans to use data analytics to bolster their cybersecurity. While analytics do require an investment up front, it's one that many experts say pays off greatly in the long run. For example, its ability to automate diagnostics and detection — and to process colossal amounts of data in a fraction of the time — reduces the energy, costs, and risk associated with undertaking these tasks manually.

Pennsylvania would agree. Beginning in 2014, its Office of Information Technology began investing in advanced analytics in order to reduce the time spent manually reviewing log files which contain information about network activity.[11]

Commenting on the leap to analytics, the state's chief information security officer, Erik Avakian, considers it a major advantage: "You've got analysts now that don't have to scour through days and days of logs. [Now], they can actually let the technology do most of that work for them. So from a cost-savings perspective it's really helped."[12] With so much on the line, Avakian understands that timing of the recovery process is especially critical. "With analytics," he says, "it's not so much about prevention, but detecting quick, detecting early enough, so that if something is going on [in] the network, or there's an intrusion or whatever, it can be investigated quickly, eradicated quickly."

The National Association of State CIOs (NASCIO) has also emphasized the major importance of analytics, calling it an imperative step toward defending against the latest multi-vector strategies unleashed by cyber criminals going forward.[13] As attacks continue to grow more sophisticated, state and local agencies would be wise to heed the warnings and begin devoting what resources they have to stronger analytics systems.

**Going Forward**

While the challenges will not be easy to overcome, they open up several opportunities for agencies wishing to double down on stronger cybersecurity measures. For one, state and local agencies can seek greater collaboration with other state and local neighbors when deciding how to respond in the event of a cyber attack. A great example is the recent announcement by the

---

[10] https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/
[11] http://www.routefifty.com/2016/04/cybersecurity-state-governments/127745/?oref=rf-topic-river
[12] Ibid.
[13] http://173.188.123.141/Newsroom/ArtMID/484/ArticleID/367/NASCIO-Issues-Call-to-Action-for-States-Develop-Advanced-Cyber-Analytics-Capabilities

National Governors Association (NGA) to form a policy academy devoted to pooling cybersecurity resources among five states: Connecticut, Illinois, Louisiana, Nevada and Oregon. According to the NGA, the cyber policy academy will be “a highly interactive, team-based, multi-state process” in which these states will develop and implement a shared comprehensive cybersecurity action plan.[14][15]

At the same time, state and local governments must deepen their investments in advanced analytics and increasing cyber awareness. However, navigating and managing these investments through in-house expertise alone may not be feasible in most cases, especially for municipal and county-level governments that are stretched for talent.

For these agencies, obtaining assistance through a managed security services provider (MSSP) is an attractive alternative. MSSPs specialize in this complementary role, working directly with agency personnel to find the best possible solution and deploying much needed expertise and analytical solutions where they are needed most. By automating their threat detection and getting incident management and response capabilities through such external providers, agencies can make up for the shortage of in-house cyber expertise and labor. Combine this external assistance with an internal focus on providing comprehensive cybersecurity awareness programs to new and veteran employees alike, and the forecast for state and local cybersecurity begins to look much more optimistic: agencies will be far more prepared to respond swiftly and effectively to the next great cyber attack.

[14] http://www.routefifty.com/2016/05/state-local-cyber-concerns/127942/?oref=rf-topic-rivere-topics

[15] http://www.nga.org/cms/home/news-room/news-releases/2016--news-releases/col2-content/states-bolster-cybersecurity.html