



NASCA

National Association of
State Chief Administrators

INNOVATIONS
IN STATE
GOVERNMENT

State of Michigan

Department of Technology
Management and Budget

2019 Innovations in State Government

Defining IT
Infrastructure



Executive Summary

It is a doubtless proposition that Information Technology (“IT”) is an increasingly pervasive concept in all facets of human activity. Procurement, both private and public, is certainly beholden to this truth. In the State of Michigan, IT is one of three sourcing categories, along with commodities and professional services. Michigan’s total IT spend in fiscal year 2018 was \$345,175,132.08, which is up 115% from just five years ago. Going forward, that spend will undoubtedly expand and increase, as most services, and a surprising number of commodities now include some form or manner of IT component.

Keeping pace with the rapid proliferation of IT is a daunting task. It is therefore a critical task when one contemplates all the inherent risk in IT procurement. Engaging the right IT personnel ensures that appropriate subject area expertise is involved in the process. Further, failure to match appropriate contractual terms to expanding technological developments is a recipe for disaster. Without the right people and the right terms involved in IT procurement, the risk of data insecurity grows.

Regardless of security measures undertaken, cyber-attacks and the resultant data breaches are frequent and exceptionally costly. By way of example, “US Federal agencies reported more breaches last year (57 percent) than any other industry sector by a wide margin, well ahead of the global average of 36 percent according to a new report.”¹ Additionally, “[i]n 2018, an average incident costs U.S. firms \$7.91 million.”²

As is evident, failing to proactively prepare for these situations can be disastrous; resulting in more than mere loss of money. As public institutions, our citizenry expects extraordinary diligence in prevention of data breaches. There are many pitfalls to avoid in attempting to achieve these ends.

In addition to proactively addressing security concerns, defining IT has had a profound impact on overall service improvement throughout state purchasing. All agencies purchase IT, but not all agencies have personnel adept at IT purchasing. By implementing this definition, the right people are engaged whenever there is a substantial IT component in any procurement.

The State’s efforts to define IT hardly seems like much of an innovation upon a cursory glance. When the project itself is examined as a whole, however, the numerous benefits of this endeavor are manifest.

Cyber security is an issue face by every state, without exception. The proliferation of IT components in traditionally non-IT areas of procurement is increasing exponentially. Threats from malicious actors – including individuals, entities, and even nations – are increasing correspondingly. As keepers of massive amounts of personal data, states are both a high value and high vulnerability targets. Since we have both a fiduciary and moral obligation to protect

¹ *US government agencies see 20 percent rise in data breaches*, Ian Barker, Tech News 2018. (Citing Thames report) (See Exhibit 1)

² *The Average Cost of a Data Breach is Highest in the US*, Niall McCarthy, Infographic July 13, 2018 (Citing IBM study) (See Exhibit 2)

our data – the data of our citizens – it is incumbent on us to develop solutions that keep pace with these threats.

Making sure that we identify IT is but one small step in this endeavor. It is, however, a critical first step, as identification of potentially missed vulnerabilities is precisely the misstep that allows data breaches in the first place. By leaving no stone unturned, Michigan has ensured that we have taken the critical first step in protecting its citizens from an ever-increasing threat.

Innovation

As many states do, Michigan classifies its procurement into a number of categories. Specifically, Michigan has three categories of procurement: commodities, services, and IT. It goes without saying that the line between these distinct categories grows blurrier every day as technology infiltrates the realm of goods and services. The number of commodities and services that have some IT component grows correspondingly. And as stated above, the more prevalent IT becomes, the more vulnerable an entity becomes.

Categorization of procurement areas used to be determined by what numeric percentage of the project was IT-based; projects over 50% IT-based were considered “IT.” In practice, tradition and whether the procurement agency wanted to engage the state’s IT professional drove the decision as well. While not ideal, this practice worked for many years; however, times have changed

Many, if not most services now have some IT component to them. For instance, services such as health care, which are a massive budgetary item, rely on IT to store and transmit massive amounts of personal data. Even commodities are subject to an increasing incorporation of IT components. A common example of this is in our office supply contracts. While the underlying products have no IT component, purchasing is frequently done through IT portals, through which ample sensitive data is transmitted. Of course, the so-called “internet of things” consists of numerous commoditized purchases that are highly reliant on IT terms.

So, the need to identify when IT is a prevalent component of any purchase should be evident. Michigan realized that it was exceptionally easy to take for granted the categorization of purchases, thereby overlooking instances where there was an IT component subjecting the State to potential dangers. We suspect that we are not alone in this oversight. By virtue of undertaking this project, Michigan has substantially addressed a major risk that could cause grave financial risks. Moreover, as a public body, a data breach has substantial non-financial consequences in that it can undermine the trust of the citizens. One could argue that this is an even greater damage than potential financial loss.

Transferability

Regardless of how an individual state procurement body categorizes its purchases, all involve some form or manner of the three categories used by Michigan. Furthermore, all states are

subject to the same encroachment from IT into other less evident realms of purchasing. It follows that the risk of breach increases correspondingly for all government entities. As a consequence, it is vital that all states recognize where they may have IT vulnerabilities.

As Michigan has already drafted both an operational definition and a matrix for determining whether IT components are present or not (See Exhibits 3 & 4), both the verbatim definition and a shareable template is readily available. The matrix is effectively a step-by-step instruction sheet for implementation. In particular, it dictates when readiness documents are required, an important step that will be discussed below. While any given state can modify these to suit their needs, Michigan believes that there is little need to do so. Data security is a universal need of all large organizations, whether private or public. There is no apparent unique vulnerability that any given public entity faces; the statistics cited above show that public entities are the most susceptible to attack, though.

Efficiencies Created

In addition to the dramatically reduced risk in massive losses from data breaches, the purchasing matrix, which is utilized not just by our Central Procurement office, but by all agency procurement, is a quick reference guide that improves overall efficiency. A process that once likely involved numerous e-mails, phone calls, and/or meetings to determine if there was an IT component has been substantially simplified. As soon as an IT component is identified, our Agency Services division is engaged. This division has IT expertise that can be utilized in making contracting decisions.

The impact of this project has certainly been felt throughout Central Procurement. First and foremost, it helped eliminate any confusions for commodity and service buyers as to when their bids had IT components. Additionally, the overall impact of a standardized definition amongst throughout the State cannot be overstated. Previously, employees in dissimilar roles – from a technician to the Chief Technology Officer – would use different terms, or have different standards as to what truly constituted IT. For obvious reasons, this is sub-optimal. The standardized state-wide definition eliminates confusion of roles and responsibilities and lets different IT specialists know when their expertise is needed and when it is not.

Further, by defining IT, agency autonomy has expanded greatly. Defining IT facilitated the platform for agencies to start making decisions earlier on in the procurement process. If you know ahead of time that an IT buy has to route through Central Procurement Services or not will allow you to plan in ways you couldn't before.

Previously, the Department of Technology, Management, and Budget (“DTMB”) was the only agency authorized to make IT purchases through its Central Procurement and Financial Services divisions. Now, agencies are able to make certain IT purchases through special delegated authority under certain criteria.

The purchasing matrix essentially helps establish these criteria by filtering types of purchases that have IT components, but don't require specific areas of expertise. It is an excellent tool for Business Relationship Managers and General Managers in assisting agencies in identifying IT components. It also allows users to know when readiness documents are required, alerting them to the need to gather legal terms, requirements, standard SLAs, etc.

It goes without saying that this expanded autonomy is well received by stakeholder agencies. Besides granting more control, it also shortens the procurement cycle at the agency level.

Attempting to measure efficiencies with tangible cost savings is difficult; this project does not lend itself to quantifiable metrics. A principled dollar value would require Michigan to not only recognize a breach that was avoided, but also to calculate the potential theoretical loss of such a breach. It would be disingenuous to even attempt such calculus. Furthermore, to be perfectly frank, implementation of this process actual increased short-term costs. By and large, IT procurements are more complex, more time consuming, and require input from more stakeholders. This project effectively makes more of our contracts subject to increased technical scrutiny, which necessarily takes more time, labor, and waiting.

However, as was mentioned under service improvement, this initiative has spawned many efficiencies that certainly have a cost saving effect. This project reduces the number of situations where IT components are later discovered for solicitations that were not bid as IT. The additional up-front labor thereby eliminates later scrambling to make such a solicitation IT compliant. Frankly, these situations typically occur when something has already gone wrong. Therefore, the added initial measures of prevention assuredly save time, stress, risk, and, of course money, in the long run. Ultimately, we feel confident in proclaiming that Defining IT yields overall cost savings, but any quantification is likely untenable.