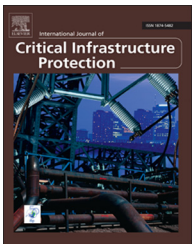
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Threats to municipal information systems posed by aging infrastructure

Ginger Armbruster[a], *Barbara Endicott-Popovsky*[b], *Jan Whittington*[a,*]

[a]*Department of Urban Design and Planning, 3949 15th Avenue NE, Room 410, University of Washington, Seattle, WA 98195, USA*

[b]*The Information School, Roosevelt Commons Building 404, University of Washington, Seattle, WA 98195, USA*

ARTICLE INFO

Article history:
Received 17 January 2013
Accepted 3 August 2013
Available online 8 August 2013

Keywords:
Aging infrastructure
Municipal data center
Capital improvement
Interdependence

ABSTRACT

State and local governments across the United States are leveraging the Internet and associated technologies to dramatically change the way they offer public services. While they are motivated to capture efficiencies, the public entities increasingly rely on information systems that are dependent on energy and related civil structures. This reliance is incongruous with the widespread awareness of aging infrastructure – decaying for lack of investment – in cities across the United States. Important questions that come up in this environment of persistent expansion of the use of digital assets are the following: What threat does aging infrastructure pose to governmental reliance on computing infrastructures? How are local governments responding to this threat? Are the solutions posed appropriate to the problem, or do they pose new and different threats?

This paper uses a case involving the disruption of a local government data center due to the failure of an electrical bus to illustrate how the threats of aging infrastructure grow, quietly and steadily, into emergencies, on par with the catastrophic events encountered in the context of critical infrastructure protection. The decisions precipitating the disruption are routine, borne of circumstances shared by agencies that are pressed to maintain services with scarce resources. Patterns of capital investment and management explain the emergence of crises in routine operations. If, as in the case described in this paper, deferred maintenance motivates public agents to explore private cloud services, then governments may solve several problems, but may also be exposed to new risks as they enter into arrangements from which they are unable to exit.

1. Introduction

Technological advances in the latter part of the 20th century, including those related to desktop and mobile devices, networking capabilities and office applications, have contributed to a significant increase in the reliance on computers to conduct daily business [12]. According to the U.S. Department of Justice [26], "the Internet is dramatically changing the way that American government serves the public. Taking advantage of the new technology, many state and local governments are using the web to offer citizens a host of services." Cities are leading the way, finding innovative ways of communicating and providing important information to their constituencies. While these important innovations are making government more accessible, they have increased the reliance on and the interdependence of the energy and

*Corresponding author.
E-mail address: janwhit@uw.edu (J. Whittington).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.08.001

computing infrastructures that support these systems. This, in turn, has increased the vulnerability to local and regional power disruptions that can affect computing and Internet availability. It has also put more focus on the need for municipalities to participate in business continuity and disaster recovery planning for their critical information technology (IT) assets.

To clarify the issues, this paper explores a recent electrical system event that affected the availability of a municipal data center. During the summer months of 2012, the municipality conducted routine maintenance on an electrical bus that supplies power to the high-rise building that houses many departments, including the data center that supports the city's networking and application services. The electrical bus incident required city managers to face the reality of maintaining aging infrastructure and the implications of the city's increased reliance on information systems.

The event itself and the final outcome have prompted the city leadership to accelerate negotiations for private cloud services. This case provides an interesting perspective about the challenges that local governments face in managing their critical and interdependent infrastructures. Among these are the challenges created when public IT and computing assets are managed by separate, federated departments subject to competing pressure for limited financial investments in infrastructure maintenance. Of primary note is the difficulty involved in managing data security and integrity across a bewildering array of lines of business in a municipal organization. Such concerns are likely to persist, even as private computing providers are brought on board, creating potential complications with regard to contracting relationships.

The seemingly minor event outlined in the electrical bus failure case study provides a lens for viewing the factors that produce colliding paths between rapidly expanding information systems and aging civil infrastructures in local governments across the United States. The analysis implicates patterns of public finance and basic methods of asset management in crises of public information systems, and ties the risks from seemingly virtuous cycles of investment in information systems to long-running vicious cycles of civil infrastructure disinvestment. The paper concludes with a critique of the city's solution to the problem of data center reliability.

2. Electrical bus failure case study

This section describes a case involving a municipal data center disruption in a U.S. city as a result of an electrical bus failure in the high-rise building housing the data center, and the reactions of the governmental departments to the problem. The case study is presented in an anonymous manner to protect the identities of the individuals involved in the incident.

2.1. *The problem*

Power to the municipal building is supplied by several high voltage electrical buses housed in units within the building (elongated patch panels that reach from the floor to the ceiling in segments). Inside these structures are layers of one-quarter inch by six inch copper plating, interleaved together at each attachment point and secured with bolts that hold the segments together. Over time and with increased use, the heating and cooling of the units contributes to expansion and contraction of the metal, which tends to loosen the bolts from their moorings. This can result in a significant increase in resistance and heat at the connection points, creating a physical "hot spot" and a potential fire hazard.

The city moved its data center to the municipal building in the late 1990s. The building was not constructed specifically for use as a data center. Rather, it was designed for regular office use and retrofitted for power and cooling. As discussed in a previous article exploring the vulnerabilities of communications collocation [4], man-made and natural disasters present regional vulnerabilities to data centers in facilities that are not built specifically for the purpose of housing information systems. Repurposing buildings that were not intended to accommodate the requirements of critical computing infrastructures presents a problem for systems management and business continuity planning.

The city was due (and perhaps overdue) to conduct a maintenance procedure on the electrical system, a procedure that should ideally be conducted every five years. During routine maintenance involving scans that included infrared monitoring for anomalies throughout the building, workers found a "hot spot" on the one of the electrical buses. The heat was so intense that the workers were concerned that the bus was contorted out of shape and may require repair or replacement. Unfortunately, this particular bus provided power to the data centers that supported city department operations. Its replacement or repair would certainly effect computing operations and city services.

2.2. *The response*

The city's immediate response was to reduce the load on the electrical bus in question. This included a coordinated cross-departmental effort to shut down all non-essential devices and lights on several floors above and below the data center. Although it was not a sustainable solution for long-term operational purposes, this approach was effective for the short term and remained in place for the duration of the maintenance effort.

The planning process to address the problem uncovered the fact that the city had, over the past decade, experienced rapid growth in the use of and reliance on information systems to conduct necessary business and communications, internally and with its constituencies. Meanwhile, the load on the buses had increased substantially because the data center had grown in size and significance.

The director in charge of computing systems was given the task of determining how to complete the repair while continuing to support the city's computing requirements. This effort necessitated the following strategic planning steps:

- Identifying the essential applications that needed to stay up.