Understanding Utility IT Services (and their Implications for Cyber Security)

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Mob: (201) 454 – 1854
eamoroso@tag-cyber.com

Abstract

Utility IT involves network and computing infrastructure support for services at layers 4 and below with an interface to business applications. Benefits of Utility IT include efficiency and scalability of infrastructure, and improved capital management. Cyber security management for Utility IT is consistent with typical security team operations and cloud migration plans. *(Analyst Note: This paper was inspired by discussions about Utility IT services with Bruce Flitcroft and Mike Funk of Alliant Technologies in April 2016.)*

Introduction

Sit for an afternoon with Alliant Technologies CEO, Bruce Flitcroft, and you'll get an earful about managed services from integrators. "I hate that business," he explained repeatedly. On the surface, this would seem an unusual statement coming from the head of a company that excelled for many years in the provision of conventional, value-added, managed network solutions for business. But the CEO was clear in his vision: "There is a much better way," he said.

The better way Flitcroft and his team at Alliant have been developing and supporting for the past few years is a new model he refers to as *Utility IT*. Inspired by the shared risk model that infrastructure providers have used to offer metered, on-demand utility power and other services, Bruce believes this new model will change the way businesses deploy IT services across their evolving enterprise networks.

Layer 4 Services and Below

The essence of the utility IT model is an underlying, high availability set of network and infrastructure services that provide a base on which to develop applications and services. By including capabilities only in the OSI stack from Layer 4 down, the idea is that businesses can buy these services like electricity – on-demand, metered, and

supported by service level agreements. The local IT team is thus free to concentrate their energies on the higher-level application services.

A key point made by Bruce was that Utility IT does not and should not include these higher-level application services. The constantly changing needs of an organization with familiar layer 7 tools such as customer databases, office support, and business applications, make utility services a much less attractive option at that higher level (see the referenced paper [1] for additional information on this point).

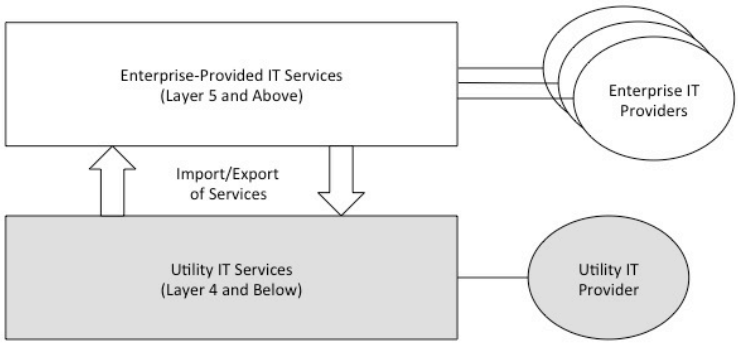

Figure 1. Utility IT – Support for Layer 4 Services and Below

The advantages of such a utility IT model are many – including greater efficiency, improved scalability, and faster agility than more traditional managed services, where equipment is placed on-premise and managed from a remote location. Furthermore, the utility model offers intense benefits for companies who desire lower levels of capitalization around their network. Certainly, this streamlined capital process places the burden on the utility IT provider to identify means for ensuing their own profitability.

Implications for Cyber Security

With the cyber threat to the enterprise increasing at an alarming rate, it is important to examine the security implications of Utility IT for layer 4 and below. The two questions to ask are first, whether the model is consistent with how existing enterprise security is operated, and second, whether the model is consistent with the evolution of security protections to virtual micro-services accessible over per-app VPNs from the mobile.

Regarding first question about existing operations, most current enterprise teams have a partitioned support model where the underlying security infrastructure, including firewalls, routers, and load balancing, is managed by a separate network team. An overlay security configuration, including security information event management (SIEM) and data leakage prevention (DLP), is then operated by the security team. This set-up is largely consistent with the utility IT model, except that the deployment of network security functions would involve export of alarms and events to the upper layers, rather than a security team doing the device management. This highlights the importance of ensuring full

understanding of the import/export interface from the utility IT services to upper layer security tools like the SIEM.

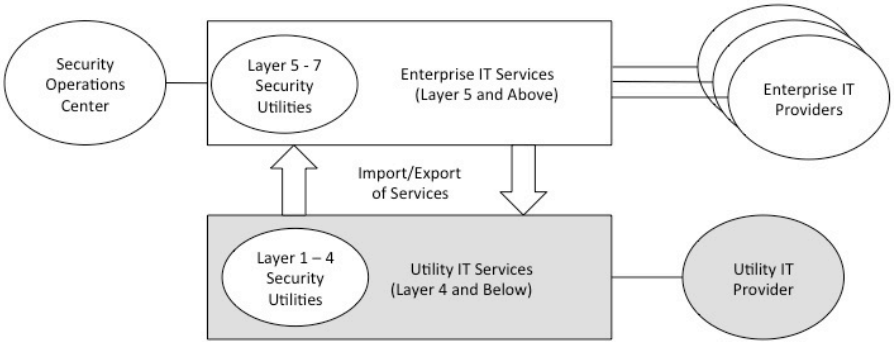

Figure 2. Exporting Utility IT Security Services to Upper Layer Tools

Regarding the second question about cloud transition, the utility IT security issues turn out to be slightly more complex. The transition from the enterprise perimeter to virtual services, perhaps stitched together in the data center and wide area network (WAN) via software defined network (SDN) services, introduces a more complicated set of compute structures. As a result, enterprise security teams desiring virtual support at the application level across hybrid cloud environments will require corresponding orchestration from the utility IT provider.

As an example, security incident response solutions hosted across several public clouds for the purpose of high availability and switchover will require the ability for the underlying utility IT infrastructure to maintain a coherent view of layer 4 and below threats. DDOS telemetry characteristics, for example, are often part of the security equation during an incident. These are often collected at layer 3, and if the data center and WAN are virtualized, then the utility IT provider must orchestrate DDOS telemetry across these virtual boundaries, which might include infrastructure support at Amazon, Microsoft, IBM, and others.

Advice for Enterprise Buyers

Cleary, this model is an evolution from the on-premise, hosted and traditional managed services model – and if you spend enough time with Bruce Flitcroft, you might begin to feel the excitement around the benefits of this new model for current enterprise networks.

A key question for most companies considering this approach will be around the financial and capital requirements associated with a transition to Utility IT. For companies such as Alliant Technologies, capital management is accomplished through creative (not in a bad way) financing and a shared risk model. But other providers of Utility IT services might have alternate means for dealing with capital, and these must be examined. Ask your provider.

As for security, the implications of the layer 4 and below protection model with exported alerts and alarms to the SIEM would appear consistent with how

most enterprise security teams currently operate. A challenge will be to make sure that the security interface between the underlying Utility IT infrastructure services and the more dynamic business application layer does not include seams where critical threat information might be mishandled or lost.

According to Flitcroft, this should be no big issue for most enterprise customers – and he is most likely correct.

References

[1] Brian Hawkins and Diana Oblinger, "The Myth About IT as a Utility," *Educause Review*, July/August, 2007.

About TAG Cyber LLC

Founded in 2016 by former AT&T Chief Security Officer, Dr. Edward G. Amoroso, TAG Cyber LLC is focused on bringing world-class, military-grade cyber security analysis, training, consulting, and media services to enterprise CISO teams around the world. The *TAG Cyber Security Annual* is its flagship annual publication, offered to enterprise security teams as an eBook or free PDF download from select cyber security vendors.