the Availability Digest

www.availabilitydigest.com
@availabilitydig

The Continuing Struggle with Legacy Systems

December 2016

What is a legacy system? Is a legacy system defined by its age? Is it defined by the fact that something (anything) new has arrived to replace it? Can a legacy system continue to be useful, or are all legacy systems bad?

The legacy systems about which we are talking are decades old, dating back to the 1970s. Several were written in languages no longer supported, such as COBOL. The software engineers that designed and implemented these systems have retired or passed away. I know because I was one of those guys (now retired, not passed away). Such legacy systems definitely are not maintainable. Yet many are still operational, and they continue to provide useful services.

Numerous legacy systems have been wrapped with modern interfaces to provide graphical user interfaces and access to modern IP networks. However, their core services remain those that were implemented long ago. They are difficult if not impossible to upgrade to provide additional services required by the enterprises using them.

Banks Are Falling Further Behind on Their Legacy Systems

Legacy systems are one of the biggest barriers keeping banks from rapidly delivering the personalized services such as those available from Apple, Google, and Amazon. Many banking systems date back decades, and they are still in use. Banking legacy services are wrapped around the staff that work with and maintain them. As these employees retire, they are replaced with younger talent who are unfamiliar with such aging systems. This attrition of staff with legacy knowledge makes it difficult to migrate to newer environments

Banks' legacy systems obstruct the movement of data between silos, preventing the 360-degree customer view that is required to provide personalized services. Banks have built layer upon layer on their legacy core systems to support new customer services such as mobile and social media. These layers make the banks' legacy systems ever more complex, meaning that banks can't move quickly. Most banks struggle to update their mobile apps on a biannual basis or to tie together customers' smart phones, tablets, and online banking experiences.

Competition is driving the digital world in a direction of anytime, anywhere access to services, data and analytics. The ubiquitous and instant access to data and insights can be realized only by open, flexible architectures that smooth the collection of data from a multitude of inputs and that share insights instantly with various devices and applications. Banking legacy systems are a barrier to achieving these goals. The complex layers of applications wrapped around banks' legacy systems slow the deployment of new products and services. The gap between the services that banks offer and that customers expect from an Apple or an Amazon will continue to widen.

To make the most of the opportunity to modernize, banks will have to replace their legacy systems. They will have to:

- remember that data is the guiding principle.
- have their data organized before migrating to a new system.
- separate staff so they can focus on the migration to the new system.
- not depend on their vendors for innovation.

This migration is being helped along by a developing industry called 'FinTech' (for Financial Technology). FinTech is composed of companies that use technology to implement financial services, to enable provision of financial services through technology, or to drive technological innovation in the provision of financial services. Some retail banks call themselves FinTechs. Others are developing customer-friendly digital services themselves. Still others are acquiring FinTechs.

It is estimated that 25% of 24 to 34-year-olds use FinTech services. This is expected to grow to 50% in the foreseeable future.

Insurers Face the Same Legacy System Battles as Banks

The biggest barrier to insurance companies adopting digital technology is their heavy reliance on legacy IT systems. They are not nearly as far along as banks in upgrading to more modern technologies. One of the problems is that insurance policies often last for decades. Old but active insurance policies are managed by the legacy systems that existed when the policies were issued.

Over two thirds of insurers run legacy COBOL applications written in the 1970s and 1980s. However, insurance companies are set to be the next wave of financial firms to accelerate their digital transformation.

Almost two thirds of the world's largest insurance companies have invested in FinTech. FinTech uses new technology and innovation to compete in the financial marketplace. One extraordinary example is wearable technology that can monitor the user's health for health insurance. Another example is the embedding of devices in cars to monitor drivers' driving habits so as to reward safe drivers with lower insurance rates. With the advent of the Internet of Things (IoT), status reports from these devices can be sent to the insurer via the Internet.

However, linking these systems to the insurers' back offices is hindered by their legacy applications. The extensive use of FinTech technology must wait for the insurers to replace them.

Legacy Systems and Security

A major issue with legacy systems is that they cannot be modified. They were developed decades ago when security was not a general problem. Therefore, they did not encrypt data in place or in flight. Today, the data managed by legacy systems is by and large not protected by encryption.

In June, 2015, the U.S. Government Office of Personnel Management (OPM) suffered a breach that affected twenty million individuals. Names, addresses, and telephone numbers were compromised, though no social security or payment card information was stolen.[1]

The OPM system was a legacy system that was too costly to move to a more secure environment. Such legacy systems are still in use in many agencies across the U.S. government.

[1] A Massive Hack on the U.S. Government, *Availability Digest*; June 2015.
http://www.availabilitydigest.com/public_articles/1006/OPM_attack.pdf

Hindered by Legacy IT Systems, Texas CIO Forges a Way Ahead

Over half of the 4,000 applications used by the U.S. State of Texas are legacy systems. More precisely, the Texas Department of Information Resources (DIR) found that 58% of its 4,130 business applications are legacy systems and present an increased risk of cyber vulnerabilities. The systems also are susceptible to unexpected operational failures.

The preponderance of legacy architectures inhibits the ability of the Texas IT staff from deploying technology that could make systems easier to use. New technology can be wrapped around the legacy systems to provide graphical user interfaces and to incorporate modern network infrastructures. However, these steps do not address the risks of the underlying legacy platforms. They are a hindrance to adopting new technologies such as IP networks, data security, and moving to the cloud.

The Chief Information Officer of Texas plans to remedy the situation. Though the cost and disruption will be significant, the State of Texas is in the process of replacing many of its more important legacy systems.

South Australia Falls Behind on Upgrading Its Legacy Systems

South Australia is the south-central state of the country of Australia. It is an example of a government that continues to rely heavily on legacy systems.

Ten of South Australia's most critical government agencies are running 226 servers still on Windows 2003, and five servers are running on Windows Server 2000. Microsoft no longer provides patches for corrections for these operating systems. Thus, South Australia has been running unpatched operating systems and applications now for years.

This dilemma is clearly a tradeoff between money and security. To provide security for its legacy systems, South Australia takes several steps. It uses application whitelisting to control which applications are permitted to be installed on a host to ensure that there are no unwanted applications or malicious code executing on the system. Only necessary ports and protocols are exposed to the network. It uses auditing and logging to monitor system activities. This data is sent to a SIEM (Security Information and Event Management) system that provides real-time analysis of security alerts generated by the auditing and logging processes.

It's Not Only Software That Can Be Legacy – Hardware, Too

It is hard to believe some of the old legacy hardware that is still in use. This observation is documented in the *Tech Republic* paper "The antique computers that just won't quit" (see the reference below). Examples include:

- A 25-year-old Commodore 65C still in use in an auto shop in Gdansk, Poland.
- A 30-year-old Commodore Amiga 2000 still in use in a Grand Rapids public school to control its heating and air conditioning.
- PDP-11 computers built in the 1970s will be used in Canadian nuclear power plants until 2050.
- A forty-year-old IBM Series 1 run by the U.S. Department of Defense's Strategic Automated Command and Control System, which coordinates U.S. nuclear forces.
- And of course, there is me.

Summary

It seems that both software and hardware legacy systems are here to stay. Even with all of their problems with respect to flexibility, maintainability, and usability, they often are simply too difficult or too expensive to replace with modern systems.

Some legacy systems have been in operation for over fifty years. What will the next fifty years bring?

Acknowledgements

A Massive Hack on the U.S. Government, *Availability Digest*; June 2015.
Legacy Systems Prevent Banks From Delivering on Digital Promises, *Bank Innovation*; June 1, 2015.
The antique computers that just won't quit, *Tech Republic*; October 13, 2016.
Insurers face same legacy system battles as retail banks, *Computer Weekly*; November 1, 2016.
Hindered by legacy IT systems, Texas CIO forges a way ahead, *TechTarget*; November 14, 2016.
SA govt's legacy IT management fail, *IT News*; November 22, 2016.
Bridging the gap between security and legacy IT, *Federal Times*; November 28, 2016.