Evolving Legacy Systems

Legacy Systems

Semi-Automatic Business Research Environment (SABRE)

AMERICAN AIRLINES

SABRE

Reservation System by IBM

SABRE Evolves

Evolving Legacy Systems

- Legacy system prioritised seat availability over all other functions.
- Information pertaining to departures, meal upgrades or even maintenance request were very slow - couple with the increase of users.
- SABRE outsourced operations ~$2.2 billion to an external organisation and sold-off legacy assets $778,000,000.
- Primary concern is not cyber security but the concern of rebel business units losing independence.

Process

Process

Evolving Legacy Systems

- Create an **inventory** of the legacy systems that exist within the enterprise.
- Prioritise and **identify high-risk legacy systems** to the enterprise.
- **Assess** identified legacy system to determine the actual level risk.
- **Define** and develop plans to evolve high-risk legacy systems.

Inventory

Process

- Essentially list all the legacy systems that are accessible to individuals and other systems.
- Creating an inventory appears trivial but can be complex, due to some systems simply going out of use.
- Similarly, some systems may be masked by modern systems but are still in use.
- Solid foundation of legacy assessment is based from a complete inventory.

Inventory

Process

- Observe the system to understand and determine the actual purpose of the legacy system.
- Research development history and understand inception, design and implementation decisions.
- Determine the type of legacy system, relevant knowledgable staff and the sensitive data as well as functions it provides and processes.
- Understand accessibility of the legacy system, i.e. open to public access, specific staff etc.

Identification

Process

- Determine the importance of the legacy subsystem to the overall enterprise system.
- Investigate the implementation and design approach adopted, understand the common vulnerabilities for any associated platform.
- Understand the development cycle of the legacy system.
- Systems are frequently developed over several years that may lack the discipline of the original implementation.

Identification

Process

- Testing approach and how security was considered during implementation.
- Type of data and the level of sensitivity, the legacy systems may be processing medical material or credit card numbers.
- Accessibility of the system in terms of employees as well as connections to external systems.

Prioritising

Process

- Verify purpose of the legacy system and information related to its development.
- Perform thorough analysis of the legacy system and understand the wider impact of the system to the enterprise.
- Understand what risks the organisations is taking by relying on the legacy system.

Assess

Process

- Assess the level of risk the legacy system represents to the organisation, much like any other risk assessment.
- The outcome of the risk assessment will influence the plan to manage the legacy system.

Define

Process

- Develop and define a plan to **accept** the legacy system or **evolve** the legacy system.

Options for Evolution

Options for Evolution

Evolving Legacy System

- Enterprises may opt to handle any concerns with legacy systems by developing **policies**.
- Legacy system can be **harden** against attackers by reducing vulnerabilities or wrapping some components.
- **Enhancing** the legacy system by developing and integration new hardware and software.
- **Replace** legacy system with alternative system to serve the needs of the enterprise.

Policy

Legacy systems

- Policies are an effective, rapid and often low-cost treatment that can be used to mitigate against the risk of legacy systems.
- Policies can be alone or can be in conjunction with other evolution options to address risk to legacy systems.
  - Policy could be used to initially address specific concerns for legacy system while a subsequent step is being delivered, such as hardening.

Harden

- **Address vulnerabilities** in the legacy system by improving software and wrapping components.
- **Restrict scope** and remain focused on the specific concern.
- **Costs** are difficult to define as may not be clear how many hours will be required to address the problems.
- Difficult to position arguments for hardening as alternative to replacing as costs are difficult to estimate.
- Software alterations can introduce further complications that could severely impact on the enterprise.

Enhance

- Many of the concerns of hardening apply to enhancement.
- Enhancement differs from hardening in that considerable software is generally added to the system.
- Functionality of legacy system components can be reconsidered.
- Enhancement affords the enterprise the option of retaining the significant investment of a legacy system.

Replace

- Costs associated with hardening or enhancement may be as significant as replacement.
- Security concerns are rarely significant enough to justify full replacement of a legacy system.
- Transitioning between legacy systems and new system will require thought and considerable planning to minimise impact.

Evolving Legacy Systems

Legacy Systems