How Midsize Enterprise CIOs Fund Legacy Modernization

By Alexander Buschek

Gartner®

How Midsize Enterprise CIOs Fund Legacy Modernization

Published 2 November 2021 - ID G00753128 - 10 min read

By Analyst(s): Alexander Buschek

Initiatives: Midsize Enterprise IT Leadership

Legacy systems pose significant obstacles, challenges and even business risks for midsize enterprises in any stage of their digital journeys. MSE CIOs must create a business case for funding legacy modernization to support digital initiatives and mitigate the risk of failure.

Overview

Key Findings

- Midsize enterprise (MSE) CIOs may not fully consider all the negative implications of continuing to maintain a legacy application or platform.
- They also may not recognize which business capabilities and integration requirements are either not supported or poorly supported by their legacy applications.
- It is generally difficult to convince the CFO and CEO to invest in legacy modernization.

Recommendations

CIOs in MSEs who run legacy systems should:

- Mitigate present and future business exposure by identifying risks directly related to running legacy systems, including security, technical and business threats.
- Build or revise their application strategy and architecture by obtaining a clear picture of where legacy applications constrain the business.
- Justify funding by presenting a business case that demonstrates business value, in addition to exposing business, security and technical risks inherent in their legacy systems.

Introduction

Many MSEs run legacy systems as their core applications, which can limit their ability to implement digital initiatives. According to the 2021 Gartner CIO Survey, 47% of MSEs are "maturing" in their digital initiatives, and 40% are initiating digital initiatives. Only 13% of MSEs do not yet have digital initiatives, a decrease from 29% in 2018. [1] Digital initiatives require a stable foundation, and as digital ambitions grow, the key systems need to change to match the ambitions.

> **A legacy system is an information system that is based on outdated technologies, but is critical to day-to-day operations.**

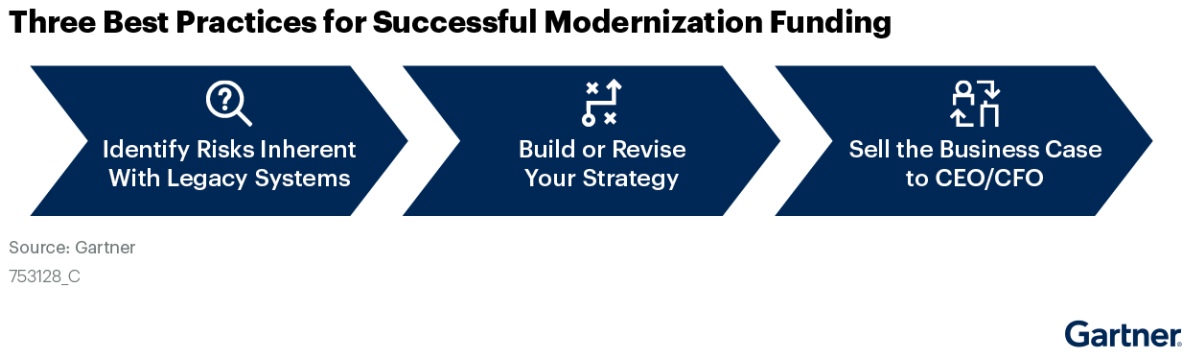
Legacy modernization will enable MSEs to move forward, while reducing business risk. MSE CIOs must justify it with a valid business case that demonstrates value. The media has reported on numerous major incidents in which legacy systems were implicated in data breaches or ransomware attacks, such as Colonial Pipeline in 2021 and Equifax. [2, 3]

And while these events draw a lot of attention, there are other legacy-system-related exposures, including:

- **Security threats:** Platforms that are no longer supported and maintained can lead to system and data vulnerabilities.
- **Technical threats:** Inability to integrate with modern applications can limit a business's ability to operate and serve customers.
- **Business threats:** Aging systems can experience technical failures and frequent breakdowns, interrupting business operations.

MSE CIOs recognize the need for legacy modernization, but getting funding for it isn't always easy. In fact, 30% of them cite budget constraints as a major challenge, primarily because their CEOs and CFOs do not recognize how legacy applications can hinder their digital business transformation. [4] Executives typically do not fully grasp digital technology complexities, such as cloud integration and API. They do, however, understand a business case. This research describes three best practices (see Figure 1) for creating and presenting an investment proposal tied to business goals and strategy that's critical to gain buy-in for legacy modernization funding.

Figure 1: Three Best Practices for Successful Modernization Funding



Analysis

Identify Risks Inherent With Legacy Systems

The most critical part of building the business case is identifying and quantifying probable risks and defining potential corrective actions to mitigate them. To ensure a thorough assessment, CIOs must involve and seek input from all impacted business unit stakeholders, as well as from the IT team. Gartner places risks into three categories: security, technical and business.

Security Risks

Identifying security exposure is a complex task, but these types of risks generally consist of:

- User privileges that have been managed poorly over a long time, allowing hackers to invade and even take over the systems
- Web interfaces that are publicly exposed and not “hardened” (see Notes 1 and 2)
- Undocumented source code
- Underlying technologies that are out-of-date or unsupported (see Note 3)
- Failure to meet compliance requirements (see Note 4).

To solve these issues, perform regular vulnerability scans and penetration tests, which are independent verification mechanisms to assess the organization's IT environment. It is also important for assessing an enterprise's ability to meet regulatory requirements and test security operations. For more information on penetration testing, see Understand the Types, Scope and Objectives of Penetration Testing and How to Select a Penetration Testing Provider. We highly recommend having penetration tests performed annually at a minimum (see Note 5).

Technology Risks

Hardware and software vulnerabilities can pose severe technical risks. For example, if you install a new ERP system, you may find out that your legacy email, financial database or custom applications aren't supported. Or, you might be unable to find someone who can support your legacy systems during a failure — or may end up paying a high price if you can find someone. Below are the most common hardware and software risks.

Hardware Risks

- Absence of a reliable hardware maintenance and support service contract with sufficient SLAs
- Lack of reliable third-party maintenance and support providers if original manufacturer support is no longer available
- Lack of frequent boot testing, documentation about rebooting and system restart procedures, particularly in emergency situations
- Absence of procedures that detail how to restore systems after a crash
- Difficulty to obtain spare parts and long time frame for obtaining them

Software Risks

- Error-prone old integration interfaces (in the absence of modern APIs)
- Inability to reinstall software on existing or new operating systems
- Lack of developers and documentation to maintain the system
- Software that still gets updates but only for features and not for security patches
- Software that no longer complies with recent standards (such as tax laws)

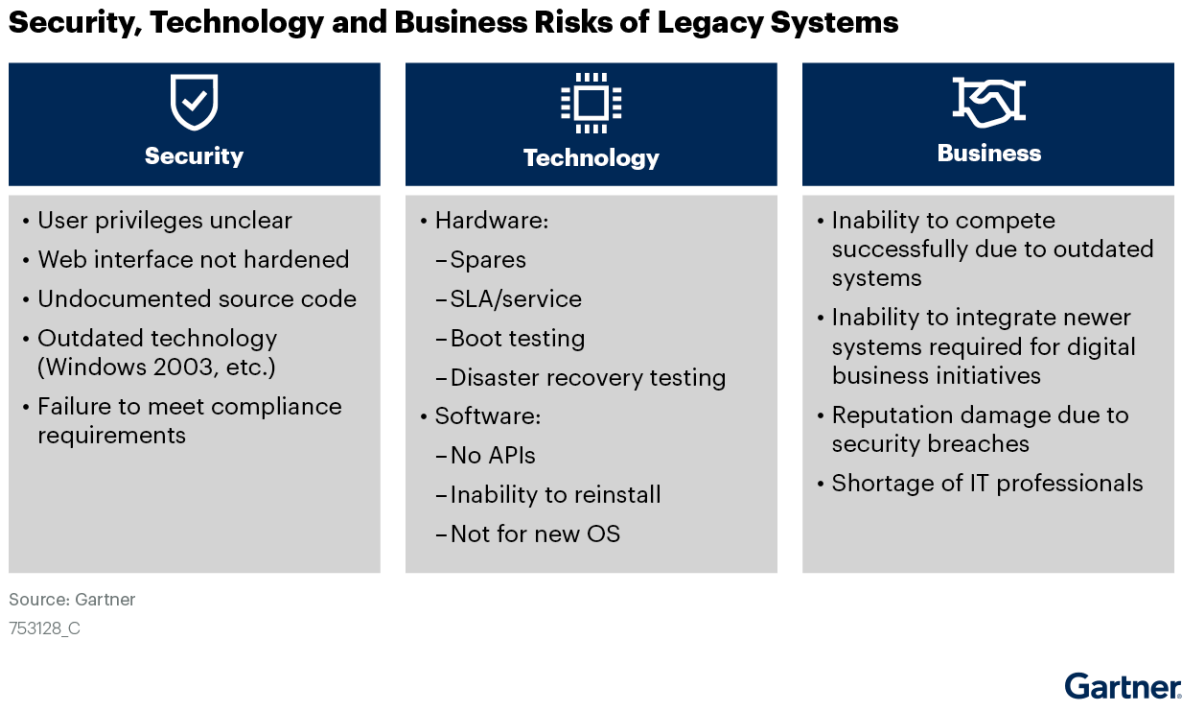
Business Risks

Business risks are directly related to security and technical risks — for example:

- Inability to compete successfully with other businesses that have more-modern systems
- Inability to integrate newer systems required for your digital business initiatives
- Business interruption caused by outages due to technical failure, such as interfaces that stop working
- Reputation damage due to security breaches, frequent outages, and other failures that lead to delayed product or service delivery
- Shortage of IT professionals with knowledge of legacy systems to support them

Aside from the individual risks, point out the associated financial impacts, including legal fees, compliance penalties and fines, costs to hire external resources, lost revenue, and ransomware costs (see Figure 2).

Figure 2: Security, Technology and Business Risks of Legacy Systems



Build or Revise Your Application Strategy

Your application strategy is the foundation of your legacy modernization effort, since it is part of the overall IT strategy, which is based on the business strategy. However, the business strategy of many midsize organizations is often communicated only verbally, if at all. It sometimes consists merely of growth figures — such as an increase in revenue in the next x years by y%. This is not sufficient.

> **A clear application strategy is the foundation of any legacy modernization effort.**

If there is no written business strategy, communicate the importance of a documented business strategy. In the absence of a strategy, justification of legacy modernization becomes obscured, as there are no viable goals to which to tie it (see Midsize Enterprise Application Strategies, Part 1 — Identify the Business Strategy).

For example, one goal in the business strategy is "to expand our business to direct selling." It is not enough to state that, "We need to modernize our ERP system to prepare a foundation to sell directly." You may find out that implementing an online store may not be possible, as your legacy ERP system may not be equipped with the APIs to integrate a cloud-based online shop. Hence, the goal cannot be achieved within the expected horizon.

The application strategy should use the business capability model as the link between the business strategy and execution (see Midsize Enterprise Application Strategies, Part 2 — Use Business Capability Modeling to Create the Right Application Portfolio).

Embrace the big picture for the organization:

- What does the organization need to do to support the business strategy (business capabilities)?
- Which applications support which business capabilities today (assessment)?
- Where do we see risk and need to replace systems (strategy)?
- What is the risk of not changing?
- How does that impact the business strategy and business outcomes?

Present Your Business Case to the CEO and CFO

First, you gathered information about risks. Then, you aligned your application strategy with the business strategy, using the business capability model. Now, you can discuss legacy modernization on a factual basis with your CEO and CFO — for example:

- You identified that the system running the ERP server is 11 years old, and spare parts are difficult to obtain. How much would a one-hour, one-day and three-day outage of the system cost? How much does it cost to obtain a backup system? How much does it cost to replace the system with a modern system? Replacing the system is necessary sooner or later. Postponing this task may add additional costs that turn out to be a waste of money.
- What is the worst-case scenario if one of the legacy systems gets hacked? What would be the organization and brand damage, and what costs would be involved to remediate it? What are the legal penalties as a result of the breach?
- How much would it cost to customize the ERP system to allow integration of a new cloud or on-premises application that is required for a new business model?

Make a business case around how much legacy modernization will cost over time. Stating that the system is too old is not sufficient.

All of these tasks lead to the risk of failure to execute your digital business strategy. It is important that all business cases are verifiable and are forward-looking. What are the consequences of running the legacy system for the next five years? How are risks changing over time?

So, how do you fund legacy modernization? Follow these three steps:

- Identify risks directly related to running legacy systems, including security, technical and business threats.
- Build or revise your application strategy and architecture by obtaining a clear picture of where legacy applications constrain the business.
- Present a business case that clearly shows business value and exposes business, security and technical risks inherent in the legacy systems.

Evidence

[1] 2021 CIO Agenda: A Midsize Enterprise Perspective.

[2] Colonial CEO Says Ransomware Hackers Exploited Legacy VPN, Cybersecurity Dive.

[3] Equifax Breach 'Entirely Preventable,' House Report Finds, BankInfoSecurity.

[4] Gartner Legacy Modernization Survey. The results presented are based on a survey to understand the stage of legacy modernization, what strategies organizations are pursuing and how legacy modernization will help to drive transformation. Gartner conducted the survey online during August through October 2018, among 659 respondents in organizations with $250 million or more in annual revenue. Respondents were screened for involvement in their organizations' core IT system modernization activities. Question: "What are the top two challenges with your organization's approach to core IT system modernization?" MSE data was taken from the survey (n = 233).

Note 1: Definition of "Hardening"

This process of identifying and treating security and compliance issues is known as "hardening." The process helps to create and maintain a secure state for systems by identifying and appropriately treating the misconfiguration, vulnerabilities, security weaknesses and compliance gaps before the system is put into production. Hardening can significantly improve system resiliency to prevailing threats in the wild. In essence, leaders are working to make things "secure by default" (see Secure by Default: Using System Hardening to Prevent Threats).

Note 2: Web-Based Systems' Vulnerability to Hackers

Whether web-based technologies and applications are public-facing or private, web-based systems are vulnerable to hackers. Newer internet technologies, such as web services and AJAX, make web development easier, but also add new security concerns for browser-based systems by making it easier for attackers to exploit any system weaknesses.

Note 3: Examples of Out-of-Date or Unsupported Technologies

Examples of out-of-date or unsupported technologies include old SQL versions, VBScript, Microsoft .NET Framework, Lotus Notes and Java. As a result, these technologies often contain known vulnerabilities that can't be corrected, leaving them exposed to systems and data attacks (see 10 Reasons SQL Injection Still Works, Dark Reading).

Note 4: Compliance Requirements

Regulations require that the technology be supported, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (DSS) and the U.S. Sarbanes-Oxley Act. Compliance audits are difficult and costly, and a data breach can set up the business for expensive fees and penalties.

Note 5: Frequency of Penetration Tests

The frequency of penetration tests depends on regulation and compliance. Payment Card Industry (PCI) calls for a test every six months. According to the 2021 Pen Testing Survey Report by Core Security, 86% of respondents conduct a test annually at a minimum.

Document Revision History

How Midsize Enterprise CIOs Fund Legacy Modernization - 9 January 2020

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Midsize Enterprise Application Strategies, Part 1 — Identify the Business Strategy

Midsize Enterprise Application Strategies, Part 2 — Use Business Capability Modeling to Create the Right Application Portfolio

Midsize Enterprise Application Strategies, Part 3 — Create the Application Strategy

---

Actionable, objective insight

Position your IT organization for success. Explore these additional complimentary resources and tools for CIOs.

Roadmap

Emerging Technology Roadmap for midsize enterprises

Benchmark your plans and make confident investment decisions.

Download Now

CIO Agenda

eBook

Peer Benchmarks for the Most Critical IT Performance Metrics.

Download Now

Roadmap

The IT Roadmap for Digital Business Transformation

Avoid pitfalls and lead smart, effective digital transformations.

Download Now

Webinar

API-First Strategy for Midsize Enterprise Business Model Transformation

Discover how you can enable business model transformation.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Gartner

Get More.

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Gartner®