kyndryl.

December 2023

Cyber resiliency and legacy asset modernization

This paper was developed in collaboration with The Asia Group.





Overview

As organizations become increasingly reliant on digital infrastructure, so does their propensity for falling victim to a cyberattack. However, one of the largest impediments to cyber resiliency is an overreliance on legacy assets retired hardware or software systems still in use. Critical infrastructure such as banking, government and healthcare are especially reliant on legacy technologies to power their critical operations. Just as with cars, the cost of maintenance eclipses the cost of purchasing new systems and the modern models come with decades of improvements and upgrades for safety and standardization. This white paper addresses three key challenges confronting legacy technologies—security risks, talent gaps and hurdles to digital transformation—and provides actionable steps for organizations to modernize their legacy systems to create a stable and secure cybersecurity base.

Challenge 1: The security risks of legacy technologies

Vendors regularly retire legacy technologies, no longer providing support or critical updates, like security patches, for the systems. As these technologies are retired, routine patching ends for new security vulnerabilities. For example, Microsoft finally ended support for the Windows Server 2008 in 2020.¹ Since then, 1,546 vulnerabilities have been discovered—an average of 327 vulnerabilities each year. The annual number of vulnerabilities discovered increased sharply after 2018, when the 2020 end-of-life was first announced (Figure 1).² Shortly before the end-of-life date, Microsoft estimated that 60% of its installed user base—over 20 million instances—were still running on Windows Server 2008 and SQL Server 2008.³

Many organizations today still rely on retired technology, leaving themselves open to more frequent and severe attacks on increasingly vulnerable systems. It's important to routinely monitor assets that are past end-of-life status for patches of any out-of-service assets. Patches released outside of a vendor's announced service life are typically intended to fix mission-critical exploits.

Often, legacy technologies also lack the required encryption standards needed to remain secure. For example, Wired Equivalent Privacy, which encrypted traffic using 64 or 128 bits, was retired in 2004. Today, this legacy technology is widely considered obsolete, yet plenty of organizations continue to rely on it.⁴ Quantum computing and other advanced computing technologies will make cracking this legacy encryption increasingly trivial. Quantum computers are even expected to crack the significantly more robust 2048-bit RSA encryption standard by 2030.

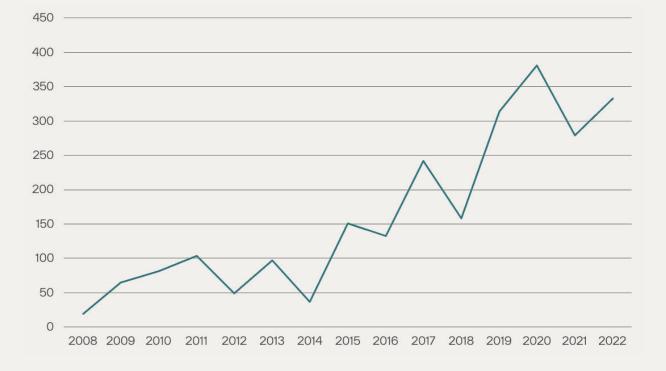


Figure 1: Number of vulnerabilities in Windows Server 2008 system. Data from CVEDetails.

Supporting tools and mainframes

As high-performance computers, mainframes often serve as the backbone for a company or government's internal Information Communication Technologies (ICT) infrastructure, offering operational security and reliability because they can process and hold large amounts of memory and data. They are often called mission-critical systems because of their size and capabilities. Kyndryl's survey of ICT companies showed that 95% of companies are moving at least some of their mainframe workloads to the cloud or distributed platforms, and moving 37% of their workloads off the mainframe.⁵ The growing economic costs of intrusions or unplanned downtime can influence a customer to consider modernizing their mainframe environment. For example, mission-critical workloads are often run in the mainframe environment where it is critical to upgrade to ensure no related service disruptions occur due to older components or middleware. Kyndryl's survey also revealed that security was the driver behind 85% of respondents' decisions to modernize on their mainframes, with almost half of surveyed companies specifically concerned about cybersecurity.5

Companies typically embark on one of three avenues to address legacy mainframe assets:

01.

Modernizing directly on the mainframe

02.

Integrating the mainframe with new technologies like the cloud

03.

Fully moving off the mainframe

Kyndryl's survey and analysis found that companies were almost universally pursuing a hybrid approach but saw comparable average annual savings for modernizing on mainframe (US\$23.3 million), integrating with cloud (US\$26.6 million) or moving off mainframe (US\$25.6 million)— which means, collectively, the organizations in our survey realized annual cost savings of US\$12.5 billion. These approaches all translated into around 10% increases in profitability regardless of method.⁵ Companies should look internally to identify which core processes would be better to run on the mainframe and which would be better suited off the mainframe. For cloud integration or greater data accessibility, integrating with the mainframe may be optimal. However, all should take care to ensure mainframes are meeting base cybersecurity standards.

The Spectre hardware exploit, discovered in 2019, and its most notable example, Meltdown, have raised questions over underlying assumptions about hardware reliability. Spectre and Meltdown exploited built-in vulnerabilities in how central processing units (CPUs) read data to access private user information and were the first large-scale hardware exploits to affect CPUs directly. Given their ubiquity, a hardware flaw in CPUs makes all of a company's electronics vulnerable. While software vulnerabilities can be addressed using patches and updates, hardware vulnerabilities cannot be overwritten in the same manner and must be addressed through operating system-level updates. Over time, this process led to technology sprawl as different permutations of operating systems and hardware required unique operating system updates. In addition, these solutions were found to significantly slow CPU processing speeds.6

While the researchers who first discovered Spectre and Meltdown initially kept their details secret until fixes could be found and deployed, future hardware vulnerabilities could be discovered and exploited first by cyberattackers. Hardware exploits may be used more frequently moving forward, given their efficacy: they are able to affect systems at a base level, vastly increasing the number of targets available to cyberattackers. Previously, companies could put legacy technology behind internal firewalls, but that is no longer a fully viable solution. Cyberattackers now go after the people and endpoints to reach the network, then circumvent the firewall after gaining network access.



Challenge 2: Finding talent with legacy programming knowledge

Organizations strive to modernize their customer experience with digitally immersive technologies. This progress can be a major challenge for organizations that rely on monolithic legacy technologies, as these systems can significantly impede the ability to quickly modernize. For instance, the organizations often reliant on legacy systems today-including banking, government and healthcare-created applications based on languages popular in the 1970s and 1980s, like COBOL, Fortran, PERL and Lisp. Since then, Java and Python have become the standard languages for next-generation technology. As a result, organizations invest considerable resources bridging the gap between legacy and modern code bases. Even if developers look to modernize their legacy systems, they often struggle to find the original source code or discover it to be poorly documented, compounding the overarching difficulty of the modernization process. This challenge points to the importance of a consistent, iterative modernization process, with a specific focus on modern cybersecurity principles rather than piecemeal efforts to upgrade legacy systems.

Finding talent who know legacy programming languages is becoming a major challenge. A 2023 survey from StackOverflow found low developer utilization rates in the past year for COBOL (0.66%), Fortran (0.95%), Perl (2.46%) and Lisp (1.53%).⁷ As programmers with knowledge of these legacy languages retire and companies hesitate to modernize, the labor supply decreases while demand remains constant, increasing both the cost of this labor and the duration of the software development cycle.

Organizations that rely on these legacy languages for their critical infrastructure are facing a costly decision between modernizing legacy applications so that they can continue to operate or continuing to spend to recruit from a dwindling talent pool. Some opt to finance highly paid developers to learn legacy languages but can struggle to find volunteers to do so, as employees know that learning legacy languages will limit their career opportunities. For example, Kyndryl's survey showed that 56% of surveyed companies were concerned that new hires did not have enough mainframe skills and 47% had concerns that staff with mainframe expertise are retiring.⁵

To meet this challenge, companies can proactively ask remaining legacy programming developers when they plan to retire and gauge if any other developers at the company would be willing to learn these languages. The company could use this information to make better decisions on timelines for modernization.





Challenge 3: Digital transformation challenges and opportunities

Legacy hardware leads to disruption

The recent semiconductor shortage, improvements in server capability and the gradual slowing of Moore's Law—which observes that computer processing power doubles at a rate of roughly every two years—have slowed server hardware refresh cycles. 49% of organizations say that they refresh their servers every five or more years.⁸ All legacy hardware should be upgraded to minimize the risk of disruption and cyberattacks. Hardware failures continue to be a main source of disruption for organizations, with a recent Kyndryl survey finding it to be the top IT risk event category among 300 ICT companies.⁹

Furthermore, the 2023 Sophos report "The State of Ransomware" surveyed 3000 IT leaders in 14 countries and found that an exploited vulnerability was the most common root cause of ransomware attacks (36%), followed by compromised credentials (29%).¹⁰ Companies can no longer rely on legacy infrastructure to keep them protected as they have in the past. This reality is further highlighted in the Allianz Risk Barometer for 2023, which found that cyber incidents (for example, cyber crime, malware and ransomware causing system downtime, data breaches, fines and penalties) are the most important business risk globally, followed by business interruption (including supply chain disruption).¹¹

Digital transformation hurdles with legacy technology

A McKinsey analysis between traditional banks-which McKinsey characterizes as frequently run on outdated technology systems designed in the 1980s and 1990s-and modern fintech companies found that modernizing systems provides financial benefit.¹² Their analysis found that fintech platforms had operating costs as low as 10% of traditional banks. McKinsey's analysis also suggests that innovative applications built on outdated infrastructure will take longer to translate to work with modern systems-delaying time to market and ceding the advantage to competitors. Kyndryl's survey found that mainframe transformation costs only 3.9% of an organization's IT budget and resulted in around a 10% increase in profitability.⁵ Employees and companies will continue to innovate, but it is more difficult to realize the fruit of this innovation if it is borne on legacy assets. Legacy languages and platforms require protracted and difficult testing and release processes, which reduces developer productivity and constrains innovation.

Actionable steps

Steps to modernize legacy ICT systems:

O1. Identify your organization's definition of legacy.

Legacy can refer to ICT assets that are no longer supported by their vendors, lack modern security encryption protection, don't have the agility for the modern needs of the organization, or are hard to support with the existing talent pool (for instance, built on legacy coding languages). Companies should assess based on their budgets and needs to determine which assets should be prioritized for modernization.

02. Map legacy assets.

Conduct a thorough review of all the ICT systems that your organization is using today to identify which assets fit your definition of legacy. A thorough review and mapping will help strategize which assets to prioritize.

03. Tie legacy ICT assets to critical business processes.

Organizations frequently delay updating legacy applications, systems and hardware because they are essential to core business operations. Understand how your organization relies on these assets for critical business processes and create an action plan to find a workable timeline for these assets to be updated.

04. Define maximum allowable downtime for core business processes.

Long-term reliability may require short-term disruption. Determine whether the legacy technology, security protocols, and backup and recovery capabilities can meet your organization's cost of downtime, recovery time and recovery point objectives.

05. Analyze mainframe needs.

Many organizations are reliant on mainframe technologies for their core business. Modernizing the mainframe can increase an organization's flexibility while providing increased security and reliability. Companies face the crucial choice of modernizing on the mainframe, integrating the mainframe with new technologies or moving applications or workloads off mainframe entirely. Companies should always keep security and resiliency in mind as they modernize their mainframes.

06. Envision your roadmap to modernization.

For legacy applications, refactoring, rehosting or replatforming can be daunting. Additionally, current inflationary and economic pressures can make meeting hardware refresh cycles challenging. Executives are often held to short-term metrics, which makes it difficult to prioritize the long-term investment of modernization. However, decision-makers will find that the investments they make today to modernize their organization will pay dividends annually and in the future, enabling them to innovate more quickly and remain globally competitive.

7. Enforce strict lifecycle management on hardware assets.

There are no security patches available for devices that are still in use past end-of-support status, significantly increasing the risk of cybersecurity issues. The government can weigh enforcement policies and subsidies to engender necessary private capital investment into modernization and cloud uptake.

10. Enforce a strict patching policy to ensure all operating systems and middleware are up to date.

Even software that is routinely serviced by the developer may need to be manually updated. Companies should create and enforce company policies for employees to ensure their software is up to date—and thus secure—by creating a strict patching policy that requires the newest version of the operating system or other software.

09. Implement regular server and mainframe health checks.

Companies should preventively and proactively check their critical hardware. Reluctance to incur upgrade-related service disruptions will lead to long-term issues in overreliance on legacy hardware and longer disruptions due to preventable hardware failures.

The role of government

Governments can assist the private sector in meeting these cyber resilience goals through mechanisms like legislation, regulations, tax credits and information sharing. Where governments are not playing an active role, companies may be lagging. For example, the U.S. not-for-profit's MITRE Center for Data-Driven Policy identified that a key impediment to U.S. companies meeting modernization goals was a "lack of [government policies] and legislation calling for focused attention to these systems, multi-year budgets to support modernization, and accountability mechanisms to ensure new systems are put in place and older ones retired." ¹³ These impediments represent some areas where governments can take proactive steps to assist companies in modernization.

Furthermore, some governments could look to other jurisdictions for specific standardization requirements. For example, the United States Government Accountability Office (GAO) often plays a neutral, intermediary role in bringing issues to its attention. The GAO's review of the Internal Revenue Service (IRS) ICT policy has been notably helpful in prodding the IRS to modernize legacy assets.¹⁴ Governments could also implement a centralized accountability structure, working with relevant ministries to promote government and private sector modernization. The European Union's 2022 Digital Operational Resilience Act (DORA) and Canada's pending legislation-Bill C-26, the Critical Cyber Systems Protection Act-also offer some workable models for standardizing and mandating minimum cyber resiliency regulatory requirements in critical ICT private sector infrastructure. These models aim to provide the private sector with the clarity and resources necessary to understand, implement and regularize strong cyber resiliency practices.

Governments can also promote these requirements internationally and push cybersecurity in areas and industries where they are leaders. For example, Japan is a leader in pushing supply chain cooperation in semiconductors, pharmaceuticals and other technologies. Cybersecurity is essential to the operation of supply chains, especially as cross-border data flows become a greater driver of economic growth. Japan can lead multilaterally to promote standardization of supply chain cybersecurity.

End notes

¹ Announcing New Options for SQL Server 2008 and Windows Server 2008 End of Support, Takeshi Numoto, July 2018

² Microsoft Windows Server 2008 Vulnerability Statistics, CVEdetails, 2023

³ Microsoft Inspire 2019: The 6 Biggest Statements From Gavriella Schuster And Judson Althoff, The Channel Company, 2019

⁴ WEP, WPA, WPA2 and WPA3: Differences and explanation, Kaspersky, 2023

⁵ Kyndryl 2023 State of Mainframe Modernization Research Report, Kyndryl, September 2023

⁶ Meltdown fix can make some machines slower—Intel, BBC, January 2018

⁷ 2023 Developer Survey, Stack Overflow, 2023

⁸ Optimizing server refresh cycles with an aging Moore's law, Uptime Institute, January 2020

⁹ The State of IT Risk 2023: Key Findings from IT Decision Makers, Kyndryl, 2023

¹⁰ The State of Ransomware, Sophos, May 2023

¹¹ Allianz Risk Barometer: Identifying the major business risks for 2023, Allianz, 2023

¹² Should US banks be moving to next-generation core banking platforms?, McKinsey & Company, July 2022

¹³ Ten Recommendations to Modernize Archaic and Insecure Legacy Applications, MITRE, May 2023

¹⁴ IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements, GAO, January 2023



© Copyright Kyndryl, Inc. 2023

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.