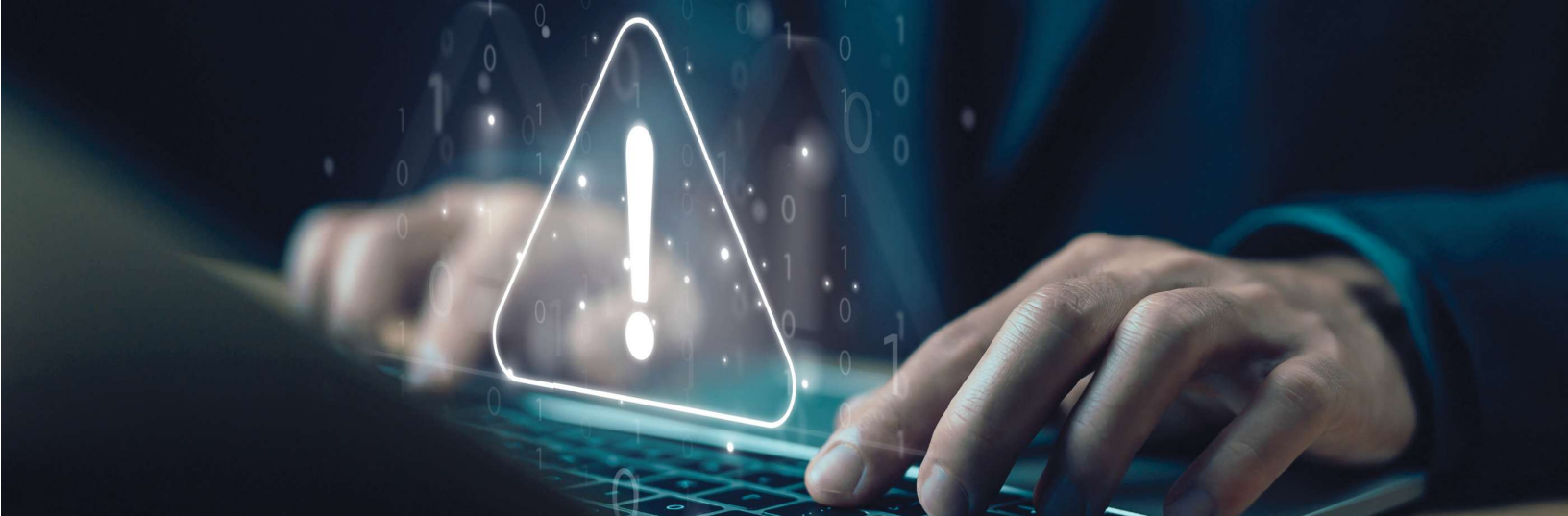




3 LEGACY TECH RISKS THREATENING YOUR BANK'S FUTURE

The ultimate guide to discussing the risks legacy systems bring to community banks and how modern core technology can help avoid them.



INTRODUCTION

In an industry where risk is a common fact of life, community banks face their fair share of it. Not only do the rise of cyberattacks and natural disasters threaten an institution, but add legacy technology to the mix and a bank opens the door to multiple risks impacting the business.

Needless to say, anyone with a fiduciary responsibility must stay alert to these threat possibilities and understand that legacy systems and their providers may not be doing enough to protect a bank. It behooves community bankers to employ every tool available to mitigate risk.

Modern core banking technology is one such tool.

A system based on modern core technology helps a community bank fight the good fight against numerous threats that raise the specter of loss. Additionally, it helps level the playing field for community banks, enabling them to provide products and services that rival larger financial institutions.

In this eBook, we will explore three potential risks associated with using legacy technology that could affect the future of your bank. We'll then discuss how a modern core banking system—in partnership with the right provider—could help a bank manage and mitigate these risks, and ultimately help “future-proof” your financial institution.

3 LEGACY TECH RISKS THREATENING YOUR BANK

Community banks operating legacy core systems risk negative impacts to their business. Here are just few of the major risks we're highlighting in this ebook.

1

Security Breaches & Data Loss

The digital advances of the last few decades have transformed the way our society does business. Banking is no exception: No bank of any size can compete in the financial marketplace without a solid presence in the digital world.

But while the rise of digitalization has created new opportunities, novel forms of malicious activity have also skyrocketed. For example, data breaches compromising confidential business information can easily result in dollar losses in the millions for a financial institution.

Community banks are especially vulnerable to these data threats. For one, many community bankers often struggle to maintain adequate IT staff that can oversee a bank's operations and mount a sound defense against cyberattacks. Because of limited resources or expertise, a community bank's internal IT team (if one exists) may not be enough to safeguard the institution.

To address these limitations, community banks often turn to their core banking provider. But ironically, relying on a provider could itself create a vulnerability. This can occur on two fronts: the quality of the core system itself; and the professional reliability of the core provider.