# CARRIERS: AVOIDING THE COST OF MULTIPLE APPLICATION PLATFORMS

ORIGAMI RISK

# 5 ways siloed data hurts your bottom line

## 1. Creates a dependency on inefficient external reporting applications

Multiple platform architecture complicates the reporting process. While third-party reporting tools can be used to analyze data across multiple systems and produce unified reports, there are costs incurred. Forrester reports that nearly half of all data professionals spend at least as much time prepping data as they do analyzing it. This inefficiency worsens in cases where reporting reveals a need to modify how data is captured or organized, forcing analysts and IT resources to trace data all the way back to its original source and then make changes.

In some cases, third-party reporting tools can also create a gulf between those who master the reporting technology and those seeking answers from the reports. In a recent interview, Christopher Ittner, chair of the accounting department at The Wharton School, discussed how this division affects the business process:

*"What we are finding is that in a lot of companies, there are great data scientists and great business people but what is missing is business people who know enough data analytics to say, 'Here is the problem I would like you to help me with.' And then they can take the outcome from the data scientists and see how they can best leverage it. That is where we must get to in the next couple of years if we want to take advantage of the digital technologies."*

Providing users with direct access to reporting that requires no prep work solves both issues. End users can become their own data analysts and answer the business questions that apply to their work. Without the requirement to master the technical process of assembling, scrubbing, and joining data from multiple systems, reporting becomes more efficient, effective, and scalable.

## 2. Impacts customer service levels

Automation is an essential tool for improving customer service. As an example, *Bring personalization to the claims process through automation* points out the benefits of a claims system that "automatically sends notifications, assigns tasks, or generates reports to make sure any claim falling outside the pre-set parameters gets the extra attention it warrants. This happens instantly, every time, meaning no claim—and more importantly, no claimant—gets overlooked." To provide this type of continuous red flag monitoring, automation must be applied consistently across entire processes.

When a combination of systems is used to handle different aspects of a process, this oversight benefit vanishes. Struggles with applying this automated red flag monitoring to a multiple-application environment could explain why nearly 80% of respondents in an IDC study stated that "gaps in automation in their existing systems—and the lack of integration between them–adversely impact the quality of the customer experience they can provide."

Silos limit the ability to utilize automation in a strategic and comprehensive manner. A single application stack, on the other hand, improves customer service by ensuring nothing falls through the cracks at any point in the process.

## 3. Preventing the migration to digital underwriting

The role of the underwriter is transitioning from an administrative role to one that is analytical. For insurers, this means a key strategic objective will be tied to how organizations manage this shift. *The challenge of digital underwriting* comments on the transition:

*"Rather than seeing the commercial underwriter as a function that will be completely automated, this view challenges the role of the underwriter itself. A Carrier Management article states: 'Accordingly, the underwriter's role as a decision maker is also evolving, with some underwriters now being called data scientists due to their use of analytics to measure and manage risk.' In this view, the value of the underwriter depends on their ability to aggregate all of the data involving a customer, and then apply perspective and judgment when analyzing the data."*

The bedrock components of the digital underwriter are agility and unfettered access to data. Third-party put obstacles between underwriters and the data they need to analyze risk. Data silos also slow down the entire underwriting process. Unless underwriters are armed with the speed and access to data required to excel as data scientists, this entire competitive strategy becomes difficult, if not impossible, to deploy.

## 4. Limits the ability to uncover insights from data

Data only has value if it triggers insights that lead to action. Ravi Mayuram, Senior Vice President of Engineering and CTO at Couchbase, writes about the effect silos have on the analysis of data in the article *Collecting Data Is Easy — The Value Is In Connecting The Dots*. "The challenge centers on the way most data today is stored. Most often, data resides in disparate databases, data silos and/or applications. This presents a major problem for organizations," he states.

Siloed data is inherently difficult to analyze. Without effective analysis, actionable insight becomes impossible. An [Alteryx study](#) indicates that "Data professionals spend 60% of their time getting to insight, but just 27% of that time is spent on actual analysis." A majority of the non-analytical time is spent either searching for data or preparing it for reports.

Mayum recommends that "these silos need to be combined in innovative ways to uncover the insights buried within." Creating a single application stack is an effective way to eliminate silos and spend more time producing insights. "By tearing down the barriers between data silos and making data more fluid and more shareable, we unlock data's inherent potential. These insights lead to countless benefits—from preventing crimes, to curing diseases, to driving business growth," he concludes.

## 5. Reduces manager effectiveness

Managers are most effective when they provide guidance and direction to their team. Unfortunately, this is not how managers spend most of their time. A [West Monroe survey](#) of 500 managers across the country found that, "the majority of managers claim they are too bogged down with administrative tasks to provide adequate feedback and direction to their team." Troubleshooting between multiple systems, as well as chasing data across multiple silos, adds to the administrative burden and contributes to this imbalance.

The solution lies in exception-based reporting, which is made possible through flexible reporting and trigger-based notifications. Dashboards indicate overall productivity and help users to visualize performance indicators. Any matters that exceed defined parameters— candidates for extra attention—are immediately flagged and escalated. In this way, managers spend more time resolving issues than dealing with bureaucracy. This directs the focus of managers to issues that have the greatest potential for impact and allows them to direct their team on appropriate next steps.

Siloed data adds reporting inefficiencies, negatively impacts customer service levels, and prevents carriers from moving to digital underwriting. Additionally, insights remain locked in data while managers struggle to devote more time to directing teams. Single application solutions eliminate these issues and drive out the inefficiencies that affect the bottom line.

# Single platforms advantages and reducing TCO

Insurance carriers that rely on multiple-vendor application stacks to manage core functions such as policy management, billing, and claims administration may be placing limits on the strategic advantage IT departments can offer. As the number of supported vendors increases, more IT resources are forced to focus on managing application stacks rather than identifying and developing competitive technological advantages.

An Ivanti survey analyzed in *The CIO's Conundrum: Can IT Move From 'Keep the Lights On' to Creative Thinking?* underscores the tension between maintenance and innovation. "In this survey, what became crystal clear was the counterbalancing of maintaining essential IT services with the desire to be bold and to act as a creativity dynamo." Matthew Smith, President, Demand Generation at IDG Communications, notes that the survey results indicate that organizations "need to liberate

their CIOs to think ahead of the curve rather than obsess over day-to-day operations. But today IT is all too often still regarded as a support function or information leaders are too stretched to drive competitive differentiation."

Sandra Gittlen writes in *Whittle down application sprawl*, "out-of-control application stacks can jack up costs, introduce vulnerabilities, add to infrastructure complexity, jeopardize licensing and waste staffing resources." This pulls resources toward the maintenance side of the spectrum and away from the strategic side. Glitten concludes, "IT's value is not in supporting technology, but in understanding the business and using technology to achieve business goals."

## The hidden costs of multi-vendor solutions

While a "best-of-breed" approach makes sense on paper, in reality it can prove an expensive path. According to the IDC report *Containing Vendor Sprawl: Improve Security, Reduce Risk, and Lower Cost*, "Mixed-vendor environments can cost 4x as much as a single-vendor environment on an annual basis." Multiple factors can contribute to this added expense.

### Integration support

The IDC report identifies the challenges involved with supporting integrated solutions:

"Integrated applications will operate together on the system, but they will still have different administration requirements, command consoles, and reporting mechanisms. Each application will require different skills and knowledge to operate the control interfaces, command structures, and data interpretation, among other issues. On a superficial but irritating level, different applications will likely use different nomenclature for the same term, consequently increasing the training costs and likely contributing to mistaken interpretations or failure to recognize similar vulnerabilities and attacks across multiple systems."

This translates into more training, increased skill set specialization, and greater challenges related to updates and versioning. Additionally, multiple vendors increase an organization's administrative burdens by creating multiple contracts to manage, each with its own set of renewal requirements, service and training procedures, and monitoring efforts. Future upgrade paths must also be coordinated between linked systems, since changes to one system may require modifications in another,

or even the need to rebuild the integration entirely. As summarized in the IDC report, "system integration is not the gift that keeps on giving; instead, it is the sin that keeps on punishing."

### Security process

Multiple vendor application stacks increase the complexity of security analysis, thereby making it more challenging to determine cause-and-effect paths when responding to potential threats. The IDC report notes this downside to security efforts:

*"All these issues make correlation among integrated applications more difficult. Beyond the cost due to extra training and operational costs associated with management, they may cause administrators to miss attacks or relegate attacks to a minor status."*

Making matters worse, the security automation tools that professionals rely on to help make the process scalable struggle in an integrated environment. Sixty-three percent of respondents in the Juniper Networks and Ponemon Institute study, *Cybersecurity Professionals Face Challenges on the Path to Automation*, say it is difficult to integrate security automation tools with legacy systems and more than half indicate that their organization must reduce the number of vendors they rely on. According to the study:

"As a result of this vendor sprawl, security practitioners are finding themselves bogged down for nearly two hours each day processing alerts, events and logs to find malicious activity, according to the study. This leaves them with limited manpower to implement critical automation technologies and results in diminishing security postures."

## Staffing challenges

The lvanti survey indicates that nearly a third of respondents have issues with retaining tech talent, and that, given the global demand, "this is a problem that is likely to last for many years, even decades perhaps, to come." An Indeed study confirms that hiring tech talent is even more difficult, with almost 9 in 10 hiring managers surveyed indicating difficulty.

Each vendor added to the application mix brings the need for new, specialized skill sets. This can further restrict the pool of qualified candidates, or require that resources be shifted to "grow your own" training programs. With more than half of Indeed study respondents admitting that they hired tech candidates who failed to meet a job description, adding multiple vendor knowledge requirements will likely make the situation more acute. When considering the total cost of ownership (TCO) for the applications used on a daily basis, insurance carriers often overlook the ongoing expense of finding and retaining talent with skills on multiple platforms.

## User experience challenges in the multi-vendor environment

Aside from the quadrupled expense cited in the IDC report, multi-vendor application stacks can also degrade the efficiencies of day-to-day users. Bouncing among the different applications used to handle multiple lines of business or core functions, such as policy management, billing, and claims administration, has a far greater impact than might be suspected. Research shows that task switching, which occurs whenever users must move between applications, carries with it expensive time and accuracy penalties. These only increase as tasks become more

complex. Even penalties measured in fractions of a second can add up to a loss of 40% of productivity for users making frequent application switches.

Aside from the productivity hit, using multi-vendor stacks can also impact the quality of service. The usage of different terms, data structures, and calculation methods can frustrate attempts to unify reporting and provide consistent, accurate performance. Having data stuck in silos also limits how insightful analysis can be. In the article *The data-driven risk manager* the author notes, "If data is spread across multiple silos it becomes impossible to provide valuable, truly comprehensive insights."

## Applying strategy to the insurance carrier application stack

In *How to fix the data integration mess*, Myles F. Suer, CIO magazine contributor, recommends that organizations "[s]tart by making investment in strategy and an enterprise architecture that can respond to the future." This includes examining the options available for consolidating functionality and simplifying application stacks.

Moving toward a Swiss army knife single platform environment, such as the one offered by the Origami Risk carrier solution, lowers TCO, improves the user experience, and frees up your IT organization to be more creative and forward-looking. The opportunity cost of missing out on those chances to innovate in an evolve-or-die environment could be the biggest hidden cost of all.

# How a single platform simplifies implementations

When insurance carriers undertake the process of upgrading critical IT systems, project timelines can drag on for years. Such a long project not only is disruptive and daunting, but also poses considerable risks. An analysis of a Gartner survey on the root cause of failed IT projects indicates, "[B]y ensuring that projects are kept small, and as a rule of thumb, not exceeding six months in duration, a much lower failure rate can be achieved."

## What contributes to longer implementations?

While every implementation faces a unique set of challenges, there are several common factors that can push out the go-live date.

### Complexity

A multi-vendor architecture, layered with isolated legacy systems and a patchwork approach to quick fixes, breeds a complex environment where any change may be difficult. The Cognizant white paper *Reducing IT Complexity to Accelerate Digital Business* notes, "IT complexity has become a critical imperative — requiring businesses to fundamentally rewire and simplify their IT estate."

Unfortunately, in such an environment, individual units may try to push forward independently in an attempt to find some improved functionality. These rogue efforts can lead to conflicting goals and a lack of coordination that further increases the complexity of the project. "IT complexity is a multi-dimensional problem that cannot be addressed with isolated initiatives," the white paper warns.

## Looking backward

When timelines stretch past the 1-year mark, organizations often wrestle with extended periods during which employees must continue working in the old legacy system, while simultaneously using its replacement. These concurrent solution approaches, however, can lengthen timelines considerably. A [TEAM Software white paper](#) notes, "This practice can be detrimental to the effort, causing the implementation period to go on longer than initially planned."

Additionally, when faced with long implementations, many organizations opt for cobbled together integrations and workarounds in an effort to minimize the potential disruption to clients. Instead of looking forward and focusing on the potential of the new solution, considerable resources are dedicated to single-use projects that incorporate the legacy system. Spending this type of effort on a "disposable" solution only adds to delayed timelines and longer periods of overlapping systems.

Efforts designed to increase this "dual life" phase, either by clinging to legacy systems or by trying to replicate, in the new system, a bad process from the old one, risk needlessly pushing out end dates. A dual-life period creates a chaotic and stressful environment for staff, threatens to tarnish the customer experience, and has the potential to impact the organization's objectives. Minimizing exposure to this condition is a critical factor in reducing implementation risk.

## Relying on customization instead of configuration

As noted in an Origami Risk [article](#), while customization and configuration are often used interchangeably, there are critical differences between them. Customization entails developers writing code to adapt a system to meet the needs of an individual customer. This approach is highly expensive, time-intensive (as every new addition needs to be thoroughly tested and adjusted), and prone to scope creep. Configuration, on the other hand, allows end-users to personalize a standard base system in a way that meets their organization's needs.

Solutions that rely heavily on customizations create lengthier implementation cycles and often replicate the same complex, difficult-to-change environment that inspired the system switch in the first place.

## Additional impacts of long implementations

While the risks associated with implementations lasting more than a year are cause for concern, the opportunity costs may be even greater. These costs include:

- Dedicated resources trapped in projects
- Strategic focus shifted to implementation challenges/progress monitoring
- Continuing outdated processes/procedures because the "new" method is too far away

Your organization needs to focus on competing for the next client, and delivering the level of performance your existing clients demand. Every resource dedicated to implementation is one less focused on your core business. The longer this continues, the bigger the drain on your operations. This adds yet another level of issues on top of the challenges that complex system implementations can bring on their own.

## The single platform alternative

Single platform solutions directly address many of the root causes that contribute to lengthy implementation. The integrated, modular approach of a single platform solution like Origami Risk centralizes data, simplifies procedures, and greatly reduces IT complexity. By shortening the steps required to reach the end goal, the system remains forward-looking and avoids unnecessary interim stages. Additionally, highly flexible and intuitive configuration options eliminate the need for resource-draining customization that requires a team of developers.

## A proven approach that works by design

Origami Risk has a track record of producing shorter implementations than most vendors. The benefits of a single platform architecture combined with a process design that is battle tested, consistent, and efficient yields compact timelines. This approach also delivers:

- Configurations and an implementation path designed around your organizational needs instead of the other way around
- Fast, hands-on feedback, instead of waiting for endless customization cycles to finish
- Critical insight that allows your organization to make informed, strategic choices about the best path forward.

The keys to shortening implementations, and reducing the headaches associated with implementations that drag out longer than a year, are found in attacking complexity, avoiding the "dual life" phase as much as possible, and eliminating customization cycles. With its single platform solution, Origami Risk can help streamline operations and design processes that better fit your organization's unique environment.

# ORIGAMI RISK

Origami Risk is recognized as the #1 software provider for the risk and insurance industry–where system and service come together. The experience and insight of Origami Risk service professionals allows for the optimization of our RMIS to meet the unique, specific, real-world challenges that each of our clients face. The result is the implementation of solutions that make big impacts and improve operations.

Request Demo

*origamirisk.com | info@origamirisk.com | 312.546.6515*