TANIUM

Put your technical debt under the microscope

A financial services guide to managing down technical debt.

Introduction

Technical debt is a much-discussed and strongly debated topic. Depending on your viewpoint, it's either a well-understood and accepted fact of business life, or it's a marketing narrative that's been dreamt up, ironically, to sell more hardware and services. Either way, it's not going away any time soon, and maybe that's the problem.

In the banking and finance industry, like most other sectors, the general expectation is that enterprise tech stacks will continue to grow and become more complex. This is notable given the wider context of a global economic slowdown and the inevitable cost-cutting exercises that have been initiated on a business-wide basis.

For IT leaders, this is somewhat of a predicament. You're dealing with more devices and data traversing the network. You're doing it with lots of legacy on-premise equipment. But you're also striving to modernize by pushing more infrastructure, services and data to the cloud. These are not short-term undertakings. This form of business transformation requires a transitionary period and, like it or not, that comes with some level of technical debt.

So, what are banks, insurers and brokers to do about technical debt while they're in this in-between state of partial transformation? Is technical debt simply the price of getting it done? Or is it a business impediment to getting it done sooner? In most cases the answer will be "both," so the question turns to how the debt is paid down and how quickly.

To address this, FSIs will need to identify which debts get paid off first, which ones are worth tolerating for a while longer and which ones are refinanced. Or, to put this in IT operations terms, which platforms, systems and applications do you keep, repurpose and eliminate? We frame it this way because IT, ops and security teams will play a crucial, hands-on role in both the planning and the execution.

In this eBook, we pinpoint the most common causes of technical debt in financial services institutions. Plus, we propose a prudent, common-sense approach to dealing with it in a manageable, predictable and precise way. Whether your tech debt is large or small, largely known or unknown, we'll help you get to the answers quickly.

Based on the experiences of several IT leaders that have dealt with transformation projects across the Finserv industry, this is your strategic playbook for paying down the debt and gathering up board-level support for whatever you do next.

Origins story

Tech debt exists because it's been a necessity and, perversely, has a value. Technologically, CIOs, CTOs, CISOs and IT ops leaders are responsible for keeping the business running and the money moving. Technology is simply a mechanism to orchestrate it all. The price of this technology is simply the cost of doing business.

To view the creators of technical debt as the villain in the piece is to entirely miss the point. Almost all tech investments at one time or another solved a problem and may even have been considered leading edge. Therefore, the origins of these 'debts' are known and accounted for as depreciating assets. What's more interesting is the expiry date on those debts. And it's here that IT leaders should focus their energies. Your CFO will thank you for it.

If we were to look under the hood or behind the curtain of the financial services industry, it's clear that technical debt exists in several areas and has a telling impact on everyday operations. Listing these out below is merely to point out that your enterprise is not alone, nor are the challenges uncommon.

Front-end bloat

Finserv, like many other transforming sectors, has been going through a bit of a spending spree when it comes to SaaS. Perhaps 80 percent or more of total IT spend (and debt) is being accumulated here. The pursuit of customer experience excellence has spurred much of this investment, but it's also created a certain amount of bloat. In many cases, these technologies become dormant or redundant — creating a technical debt that lives on beyond its service life.

Back-end neglect

It's reasonable to assume that 10 percent or less of a bank's IT budget is responsible for a lifetime of technology choices. All the servers, data centers, workstations and devices. All the applications, appliances, APIs and scripts. Everything that connects to, or runs on, the network. Consequently, any conversation about technical debt needs to reflect what's happening on both the front end and the back end.

Poor visibility

Finserv firms are good at knowing where the money is. What they're less good at is knowing where their data and technologies are. The overall growth in the IT estate is one reason for the lack of asset visibility and there's an argument that this could worsen as technologies shift from on-premise to the cloud. This becomes a technical debt issue if the business is paying for services that it can't see. It's also a growing compliance risk, given the ever-tightening data privacy regulations and governance over data collection, storage and processing.

No single source of truth

Data is good — except when it's dated, degraded or disputed. In most organizations, especially those that commonly debate the veracity of data, this is a symptom of technical debt. Finservs suffer this more than most, thanks to the deliberate separation of reporting functions to meet audit and compliance needs. This fragmentation means that a single source of truth is harder to come by and decision-making is made more difficult.

Telescopes, microscopes and horoscopes

To effectively manage technical debt without disrupting daily operations or compromising future modernization programs, FSIs need a plan for the plan. This starts with auditing what you have and setting milestones based on the business's established need for tackling technical debt in the first place.

Financially speaking, cost and asset reduction may be the primary driving force. Operationally, efficiency and productivity improvement could be another motivation. Strategically, the business may simply want to become more agile and innovation-led. This is why technical debt needs to be tackled from the top down.

Once known, it's time to pull out the viewing instruments and see the size and nature of the technical debt problem (including its causes). Whether it's misconfigured servers, poorly integrated applications, unpatched endpoints or unused licenses — you need an ability to focus and track everything that traverses the corporate network.

So how do you find focus? The analogy of telescopes, microscopes and horoscopes may be helpful here. Telescopes give you the big-picture view of the IT estate. Asset discovery tools are useful for that.

Microscopes give you a picture of what's happening inside the application or on the device. Endpoint management tools are vital for that. Finally, you have what a horoscope gives you. Signs, signals and — well — speculation. Needless to say, your gut instincts will do just fine.

But the horoscope analogy is not a flippant one. As previously mentioned, data points are often disputed by different teams, disciplines and layers of the organization. The prevailing mentality of "my data is right, yours is wrong" has persisted for far too long. If you have multiple, disputed sources of truth, you're essentially relying on a horoscope reading.

The argument here isn't about non-critical, innocuous or trivial data. The vast majority of corporate America has no idea about basic operational facts, such as how many endpoints they have. They know even less how many software licenses they're running or how many devices are unpatched and open to the internet.

To have any hope of tackling the technical debt mountain, IT ops teams need a telescopic and microscopic view of the entire IT estate — from the network to the endpoint.

Big bangs and pulse stars

Technical debts are not created by Big Bang events. Contrary to what many think, the biggest technical debts are not caused by singular investments in monolithic, proprietary platforms. In many cases, these technologies will help with visibility and control of the IT estate. Even if it comes at a premium.

More commonly, a firm's technical debt pile will have been accumulated over a long period of time. They're the result of a lifetime's technology choices — and not all should be considered bad. Afterall, some technical debt is necessary in the short term. It keeps things running along. It keeps problems off the radar.

Bad technical debts on the other hand have something in common: a failure or an inability to pull the trip switch. These are not the historic investments that an FSI may be actively depreciating, such as an on-prem data center or a custom-built application. No, we're talking about the unknown, uncontrolled technical debts such as the number-one culprit — unused or underutilized SaaS licenses. But it also includes the whole gamut of redundant assets, such as servers, devices and endpoints that haven't been decommissioned or patched.

This is where you can put the biggest dent in the debt. This is where the "keep, repurpose or eliminate" strategy needs to be deployed. Any unknown asset in your tech universe is effectively acting like a pulse star — constantly emitting "radiation" as it burns through your cash and your perimeter defenses. Unlike the big mainframe investments of yesteryear, these costs live on indefinitely and are more of a threat to the business when you factor in the regulatory risk.

In many cases, it's a contest to discover the unaccounted-for assets first. It's a sprint to map the size of the technical debt problem and all its inherent risks to the business. It's better that you win the race, rather than the audit team or regulator.

But tackling the debt and solving all the IT estate's shortcomings in one Big Bang is impractical and unrealistic. Getting all the pain out of the way in one go is what causes technical debt to persist. The pain isn't tolerable and it's not a project people want to tackle on their watch.

A heavily staged approach would work much better and better satisfy the stakeholders at the top of the food chain — especially the CEO and CFO. After all, no business leader is going to come to you and say: "Hey, let's reduce our technical debt." They're looking at the ongoing and future impact of technical debt in terms of the big-ticket items: revenue generation, cost reduction, productivity, risk and competitiveness. They're interested in looking through the telescope, not the microscope.

Cleaning house

Whatever your reasons for tackling technical debt, endpoint data has to be placed front, middle and center. The only successful way of separating the technologies you need from the ones you don't is to improve your lines of sight across the IT estate, but especially at the edge of the network where the visible, actionable data exists.

For this, you need to identify every IP/MAC address connected to your network and determine whether it's managed or unmanaged (putting internal politics aside). In most cases, the business will still underestimate the actual figure by more than 20 percent.

That's often due to the inadequacy of current tools and conflicting datasets. But what's inarguable is that no CFO wants to hear that their security and compliance report has a 20 percent margin of error. That sets off red flags and, in the real world of IT ops, prevents net new funding for people and projects. All the more reason to make sure you have a clean bill of health — with a forensic-level view of endpoint visibility.

> **"CIOs reported that 10 to 20 percent of the technology budget dedicated to new products is diverted to resolving issues related to tech debt. More troubling still, CIOs estimated that tech debt amounts to 20 to 40 percent of the value of their entire technology estate before depreciation."**
>
> McKinsey

BUSINESS GOAL 1

Risk and compliance

Data regulations are particularly problematic for IT ops teams. The rules change regularly, they overlap, and they conflict with one another. Change can be maddeningly disruptive, whether its Sarbanes Oxley (SOX), the California Privacy Act, GDPR or Gramm-Leach-Bliley. You can be compliant one day and not the next. The segregation of auditing and patching activities only adds to the complexity. Converged endpoint management is a prudent way for Fintech firms to keep on top of it all because it gives all three IT domains – IT ops, security and risk – a single source of truth. In every field of expertise there will always be favored tools with specific features and functionality. But when it comes to data hygiene — the unifying goal — one common toolset is better than many.

BUSINESS GOAL 2

Merger, de-merger, acquisition or disposal

It's one thing to operate with technical debt. It's quite another to, unknowingly, pay a cash sum to acquire a technical debt. But that's what happens in most M&A scenarios. The buyer takes on the seller's assets, debts and anything left undiscovered at the due diligence stage. The reverse is also true. No seller wants to dispose of assets that could compromise its business going forward or negatively impact the deal. In both scenarios, endpoint management tools are increasingly being used to quantify the size and nature of the digital estate, which is an important marker of both risk and value. Even long after a deal is complete, ongoing asset discovery, inventory and management is essential to ensure that business entities are integrated or decoupled fully.

BUSINESS GOAL 3

Modernization and transformation

Increased technical debt adds to the complexity of software, making it more difficult and expensive to support and develop further. This is clearly front-of-mind in today's Finserv sector where so much innovation and disruption are occurring. The major banks, brokers and insurers can't afford to divert new-project spending to resolving issues related to tech debt. By reviewing the tech estate and identifying areas of overconsumption or underutilization, Finservs can remove these "sunk" costs and release funding for those roadmap projects. Technical debt can also be a talent retention issue. The more antiquated the code and tools the firm maintains, the more it inhibits the developers' ability to build new applications and competencies.

Finding focus in the last mile

Tackling tech debt in the last mile (at the endpoint) is what Tanium does really well. We work with FSIs across the country and internationally to tackle many of the business issues created by technical debt. We help IT, security and risk teams get closer to a single source of truth for applications, technologies, data flows, and their life cycles. And we do this for major players in commercial finance, retail banking, brokerage and insurance sectors.

Many of our senior executives have direct client-side experience of running teams just like yours in situations just like yours. Mergers, acquisitions, security breaches, cyberattacks, business transformation — we've seen it all and, most important, have the playbook to help guide you through.

> **"Much of IT employees' time is spent managing complexity rather than thinking innovatively about the future."**
>
> McKinsey

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.