Hidden Costs in Application Maintenance: **How Proactive Agencies Win**

Table of Contents

Introduction: Agency Differentiators

In today's digital age, it’s a given that software and web development agencies of all sizes can deliver valuable solutions to their customers.

However, even with the latest technology - AI driven or human - agencies still struggle with what happens after a project is completed. This leads to serious and hidden problems, unexpected costs, and a higher risk of customer churn.

The maintenance phase of a software project is cited as being the **longest and most expensive** part of its lifecycle, with maintenance costs rising, the older the software [1]. But when agencies are similar in terms of quality and price, what sets them apart?

This paper looks at the business side of software development in an agency context. It explores how a reactive approach to maintenance hurts agency bottom lines and its relationships with customers. It presents a data-driven approach to turning maintenance into a strength rather than leaving it as a weakness.

1. https://idealink.tech/blog/software-development-maintenance-true-cost-equation#toc-2

Maintenance is a Blind Spot

Agencies are tasked with protecting the reliability, security, and performance of the software which powers their customers' businesses. Yet many treat maintenance as a secondary operational task rather than as a first-class business function. Across agencies, three systemic challenges persist.

The consequences of each leads to; delayed upgrades, unplanned outages, budget overruns, and client dissatisfaction. In an industry which prizes quality, poor maintenance practices actually erodes it, alongside operational confidence and long-term revenue.

The Economics of Blind Spots

For most agencies, maintaining existing projects takes up a significant portion of time and resources for both engineering and non-engineering roles, amounting to **thousands of dollars**, just for a single project. [1]

When **Gartner research** says that company leaders continue to struggle to reconcile real-world cybersecurity events with negative business outcomes, agencies would do well to take note. [2]

However, many agencies don't plan or budget for maintenance in a strategic way (or even at all). This leads to inefficiencies at best and at worst **unexpected costs**, **customer churn**, and **reputational harm**.

These costs only account for the direct time spent on maintenance as entered by staff via e.g. timesheets. They don't include indirect costs, such as the time spent switching between tasks, delayed deadlines, and unplanned emergency fixes.

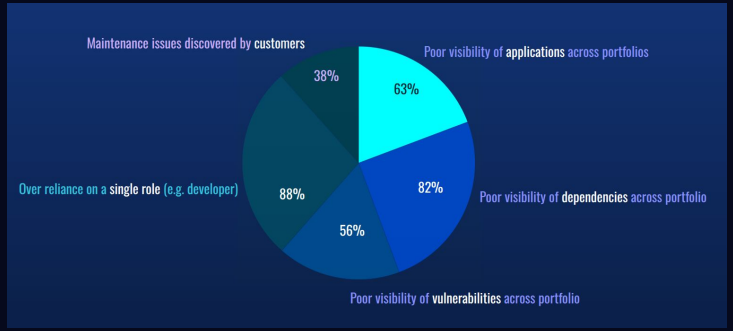
For even a medium-sized agency, the cost of not having a maintenance planning strategy can add up quickly - hundreds of hours of wasted time and resources every quarter.

1. https://www.herodevs.com/blog-posts/the-economics-of-ignoring-end-of-life-software-a-real-cost-breakdown
2. https://www.gartner.com/en/newsroom/press-releases/2025-11-24-gartner-survey-finds-90-percent-of-non-executive-directors-lack-a-measure-of-confidence-in-cybersecurity-value

Visibility - The Strategic Opportunity

Modern agency customers no longer view maintenance as optional.

Security expectations, compliance obligations, and uptime guarantees are now baseline requirements for buyers in tenders and Request For Proposals (RFPs). For agencies lacking in any way, there's opportunity to reposition maintenance as a source of competitive differentiation.



source: Agency survey 2025

Proactive maintenance also drives predictability. When maintenance risk is surfaced early, agencies initiate maintenance and budget conversations in advance. But predictability depends on visibility and that requires team-wide access to the right information. The key question agencies then need to ask themselves is:

Can our people quickly access the right data, at the right fidelity, to mitigate security and maintenance risk?

Reactive vs. Proactive Operations

Scenario A: The Reactive Agency

A mid-sized web-development agency manages fourty websites and web-applications on behalf of its customers. End-of-life (EOL) notifications are ad-hoc, surfacing irregularly often via developer-only Slack threads or customer bug reports. When a security vulnerability is published, the team scrambles to identify the affected projects. Developers are required to context-switch from billable work and project managers need to scramble to re-scope budgets accordingly.

Customers perceive chaos instead of competence.

Scenario B: The Proactive Agency

Another agency of comparable size maintains a living project inventory which tracks and notifies on End-of-life (EOL) dates, security vulnerabilities, and SSL certificate expiries for all of its customers' projects. When a key component like an application framework announces an end-of-life date or when new security vulnerabilities are published, the system immediately flags the affected app(s) and notifies the team.

The agencies' project managers prepare upgrade schedules, re-forecast budgets, and communicate the next steps to their customers before issues escalate. Developers remain focused on billable work and maintenance conversations become predictable, not panicked.

Summary

The contrast highlights the productivity dividend of proactive visibility: fewer emergencies, lower stress, and stronger customer relationships.

The Case for Metaport: Maintenance Intelligence in Practice

To operationalize proactive maintenance, agencies need integrated visibility. This is where Metaport, a platform from Dcentrica Solutions, illustrates how analytics and automation can reshape digital delivery economics.

Metaport is designed for agencies. It’s value proposition and feature set, stem from agency-specific experience.

Metaport consolidates maintenance data into a single dashboard view for use by any technical or non-technical team member. It enables project managers as well as engineering and security roles to:

- Visualise end-of-life (EOL) timelines across components like software development frameworks
- Identify customer projects affected by new security vulnerabilities
- Automate monitoring for both AI and human generated code
- Report maintenance issues directly into existing project management tools
- Import upgrade reminders directly into shared calendars

The outcome of maintenance intelligence is **operational control**: project managers front-foot upgrade discussions, developers stay focused on billable work, and executive leadership gains confidence that maintenance risk is quantified and managed.

Business Outcomes

Agencies which decide to implement structured, data-driven maintenance processes can expect a reduction in unplanned maintenance costs.

In competitive procurement environments, demonstrable maintenance maturity increasingly determines whether teams win or lose long-term contracts.

From Cost Centre to Growth Lever

The industry's old reflex of treating maintenance work as "the work after the work" is now firmly outdated. In today's digital economy, proactive maintenance is a core operational pillar underpinning security-first delivery, platform resilience, customer trust, and ultimately long-term profitability.

Agencies that invest in full lifecycle visibility position themselves to operate with foresight rather than hindsight and shift maintenance from a reactive cost centre into a predictable, revenue-stabilising discipline and a strategic differentiator.

As data breaches, supply-chain vulnerabilities, and website defacements become routine occurrences, costing organisations globally **millions of dollars** in remediation, downtime, and retrospective maintenance, the notion of maintenance as being optional is no longer tenable.

- **Log4Shell (2021, Global):** A critical open-source vulnerability impacting **100+ million** applications and devices worldwide.
- **Medicare Breach (2024, Australia):** A compromise of sensitive data affecting **12.4 million** individuals.
- **Shai Hulud Supply-Chain Event (2025, Global):** Over **700** open-source packages impacted, highlighting systemic dependency risk.
- **ManageMyHealth Leak (2025, New Zealand):** Exposure of **120,000** personal health records, reinforcing the stakes of platform governance.

These events reflect a broader reality: in a landscape defined by persistent threat activity and accelerating software complexity - especially with the advent of agentic AI - proactive maintenance is no longer discretionary, it's a baseline requirement for operational continuity and customer confidence.

Next Steps

To advance your organisation's maintenance maturity:

1. **Assess current state:** How visible are your dependencies, EOL timelines, and security vulnerabilities?
2. **Quantify opportunity cost:** Calculate the hours and margin lost to unplanned maintenance activity*.
3. **Explore maintenance intelligence tools:** Platforms like Metaport are emerging to centralise visibility and automate portfolio monitoring.
4. **Reframe in leadership language:** Present maintenance as risk mitigation and margin protection, not simply a technical necessity.

For more information on the research underpinning this paper and to explore how Metaport enables predictive maintenance visibility:

- Visit: getmetaport.com
- Watch the how-to videos: https://youtube.com/@metaport
- Review the demo: demo.metaport.sh
- Contact Dcentrica at hello@dcentrica.com

* Use tools like isitendoflife.com

About Dcentrica

Dcentrica Solutions developed the Metaport platform to bring clarity, control, and intelligence to digital delivery.

Our mission is to equip agencies with the insights to maintain, secure, and evolve their customers' solutions with confidence. Metaport is our contribution to raising the standard of software maintenance across the agency-driven web, application, and SaaS industries.

Russ Michell
Founder // CEO

Tasia Stace
Director // CFO

Luke Percy
Co-Founder // COO