Before the bubble bursts

Tackling the threat of a global security debt crisis

Orange Cyberdefense

orange™

Facing security debt

“If a builder builds a house for someone, and does not construct it properly, and the house which he built falls in and kills its owner, then that builder shall be put to death.”

Code of Hammurabi
1792-1750 B.C.

In ancient Babylon, King Hammurabi issued the first known example of a codified set of rules to govern citizens’ behaviour. Among the 282 laws, he dictated – in rather brutal terms, characteristic of the time – that those who build are fully responsible for the safety of what they build.

Nearly four thousand years later the underlying principle remains true: IT must be accountable for what we build.

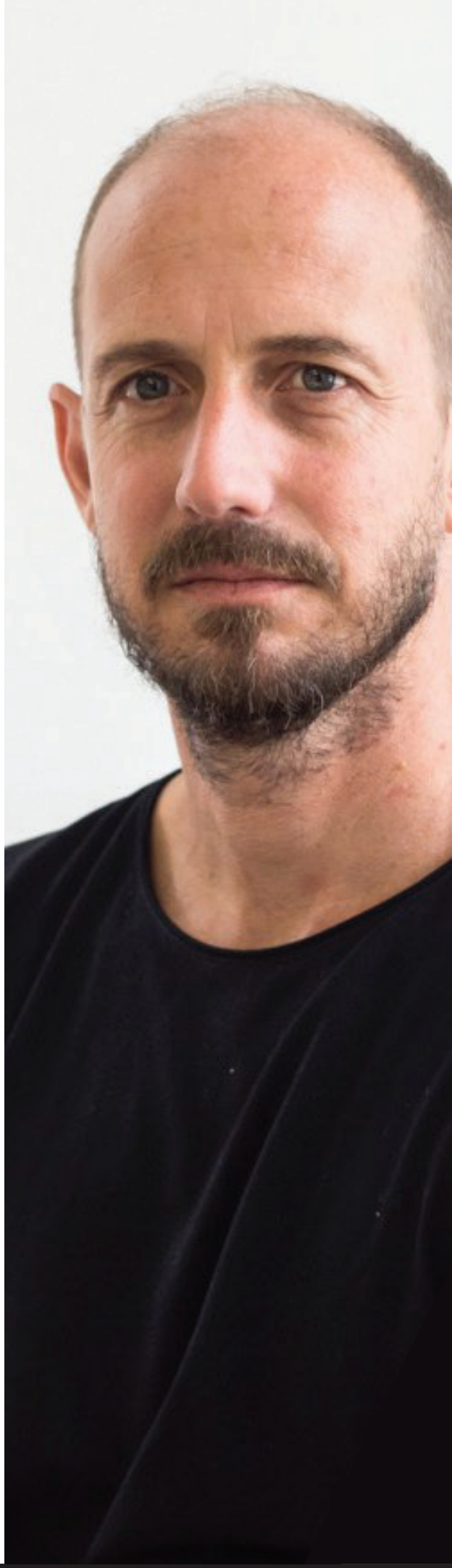
We face a looming debt crisis. I’m not referring to the $58 trillion in public debt held by governments across the planet. Nor am I referring to the $6.3 trillion debt load for U.S. corporations. Instead, I’m referring to a more intangible, but no less insidious, form of debt that threatens governments, corporations and private citizens globally: security debt.

Security debt is a derivation of the concept of ‘technical debt’ (also known as code debt), popular in software development circles. Technical debt is a term that refers to increasing the future cost of code maintenance because of design trade-offs made in the past. This concept applies neatly to security, where developers and IT teams continually compromise on the security of their software and systems.

In the quest to ship fast, bugs and other imperfections are introduced into code & architectures with a vague intention to patch or rectify in future. Done on a grand scale this technical debt can build into a security timebomb, with little or no collective planning or coordination on dealing with the consequences.

In this paper, I will make the argument that allowing security debt ‘interest’ to accrue is as irresponsible as the actions of financial institutions during the Global Financial Crisis, and could have equally cataclysmic results. I will detail the specifics of the problem, explain why the industry and wider stakeholders should take it seriously, and appeal to IT leaders and their teams to take accountability for their own security trade-offs… before the debt bubble bursts.

Charl van der Walt
Chief Security Strategy Officer
Orange Cyberdefense

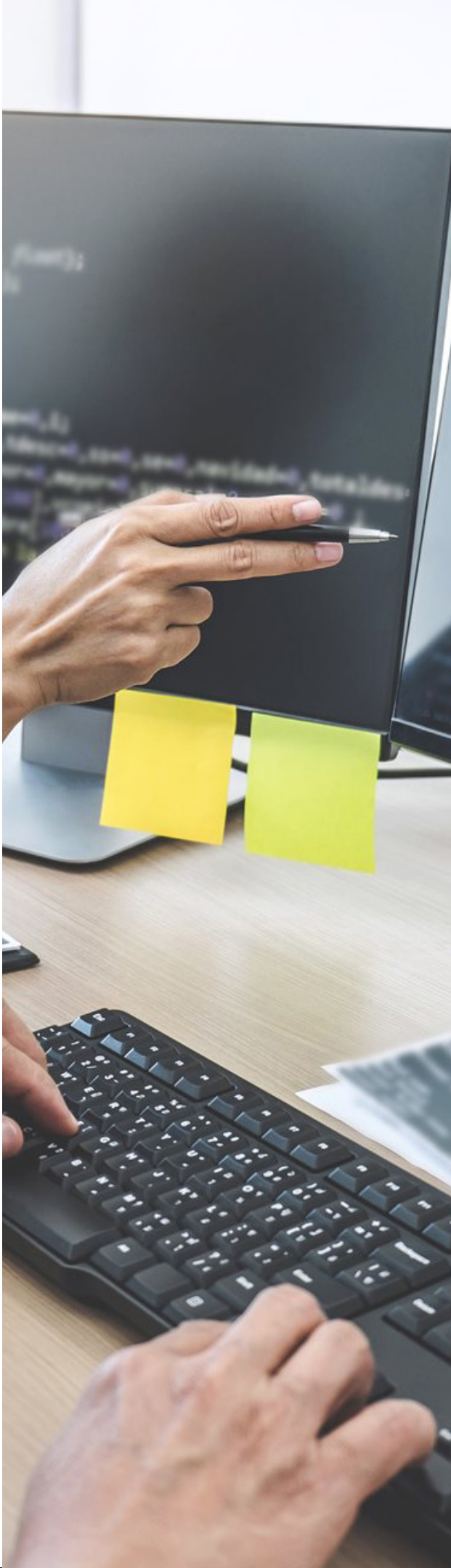


Introduction

It doesn't matter which sector your company operates within or how much data it holds: risk is ever-present.

Instead of viewing this as an endless battle, though, there's an opportunity for businesses to assume control by taking a proactive approach to cybersecurity. Many businesses are needlessly exposing themselves and their employees to risk, due to poor password security, a lack of cybersecurity skills, and choosing convenience over security.

These challenges were the subject of a recent roundtable event held jointly by Orange CyberDefense, a managed security, threat detection and threat intelligence services provider, and Okta, a specialist in identity and access management. The event gathered CTOs and senior figures from a wide range of public and private sector organisations to discuss how users can authenticate securely, and how best to create an environment that encourages digital transformation without exposing a business to unnecessary risk.



Part 1:

Lessons from the global financial crisis

Following the recession of the late-2000s, certain phrases became prominent in popular discussions. Increasingly, political and economic commentators spoke of the 'moral hazard' that had caused the crash – the idea that the financial institutions dealing in risky derivative assets were shielded from the effects of their recklessness. Further, there was greater awareness of 'systematic risk' – the unexpected consequences of expanding mortgage credit that served to have a 'contagion effect' on seemingly unrelated sectors like automotive, manufacturing and consumer goods.

These terms will long be used to explain what can happen when business leaders and policy-makers are ignorant to macro-level risks, and will be invoked to hold financial actors accountable for their irresponsible behaviour. The issue, however, is that the most serious risks are often hidden in plain sight, created without being properly understood. As the financial system grows more complex, the risks compound and can appear in unanticipated places. It's little wonder, therefore, that many economic 'doomsayers' believe a second global crash is inevitable.

IT systems are also complex and interconnected with emergent properties and, like financial systems, those risks are poorly understood and have the potential to create a contagion effect.

The question, as it pertains to this paper, is: do the risks that could trigger economic collapse necessarily have to come from within the finance sector?

Part 2:

A looming security debt crisis

The software industry, to put it mildly, is massive business. According to Gartner, the global IT market sits at $3.7 trillion and is growing year on year. Software is pervading every industry along with nearly every area of our personal lives.

Yet, perhaps owing to the exponential growth of the industry over recent decades, global regulation and governance has struggled to keep pace.

It's understandable; even the most informed minds find it difficult to predict what the future of the industry will look like, and so there's inevitable disagreement on what form preventative measures should take. More so, software development is subject to 'second- and third-order consequences' – every action has a consequence which itself has a consequence that may counteract the developer's original intention. These outcomes are by their very nature difficult to foresee, and even harder to resolve after the event.

The fact remains that the industry – either unconsciously or even intellectually dishonestly – is taking on debt at an irresponsible rate and hiding it from stakeholders, such as their customers, regulators and the wider public. In an industry constantly rushing to 'always be shipping' new code and products, the risk is compounding fast. As there is no formalised framework to measure or regulate the industry's behaviour, the problem is growing both silently and exponentially.

To provide an example of how this is playing out in practice: a development team working on an enterprise Database Management Platform may rush the coding process to meet a tight deadline for their first full release. Deficiencies in the code may be acknowledged at the time, with the intention to patch or repair potential bugs in the next release. If priorities change, or indeed the development team itself changes, those bugs may persist and become embedded in the code. With every release, more code is added like a ball of rubber bands.

The deficiencies, however, remain in the source code and become too difficult to fix. As the software receives greater adoption, the vulnerabilities – if exploited – could result in many organisations being affected at a great cost.

Now, imagine this scenario on a grand scale with potential flaws existing across suites of standard applications and software services. This is exactly what's happening every day; security debt is being undertaken but not paid back. As we've seen with major network hacks such as WannaCry and NotPetya, it only takes one exploit to have a contagion effect over entire industries and economies.

Research by the Cambridge Institute of Risk studies models just such a scenario and suggests that in the worst case the economic impact could compare with that of the Global Financial Crisis.

The bubble is growing and one day it might just pop. The effects could be devastating, not only in terms of the serious financial consequences, but also in acting as the straw that breaks the camel's back in inducing severe – and potentially counterproductive – regulation for the industry.

Part 3:

Solving the security debt threat

The responsibility for addressing the security debt risk cannot be left to policy-makers. It needs proactive self-regulation from within the industry, combined with an inclusive and collaborative approach to working with stakeholders from outside, to create awareness of the risks.

Within the industry, software companies, their developers and the businesses that use their products, all need to be committed to repaying their debts.

When interacting with those outside the industry, there must be a greater commitment to speaking the same language as influencers and decision makers. Assume that a company CEO doesn't spend time on GitHub or attend Hadoop meetups.

Assume that the CFO isn't conversant in internet-speak such as pwned, l33t and haxor. Assume that the government regulator doesn't know the ins and outs of agile development.

Speaking in the wrong terms is preclusive and can serve to repel rather than engage those that have sway over the industry's future. Clear and accessible language, on the other hand, can bring debate and foster greater understanding of how software development works, and what can be done to limit and address unintended consequences.

Tackling the threat: 5 recommendations for it leaders

Threat 1

Integrate greater security measures into the software development lifecycle, with clear responsibilities for checking code security throughout the process.

Threat 2

Commit to fixing past code errors – no update should be released without having paid off at least some 'debt' of the previous release.

Threat 3

Be proactive in starting conversations with stakeholders. Don't wait for regulators to come to you.

Threat 4

Critically assess the way you talk about software development. Jargon-filled, niche language can serve as a barrier to engaging stakeholders. Simple language and clear analogies, on the other hand, can spark debate.

Threat 5

Start now. Software fixes only grow more ingrained and harder to fix. Identifying flaws and vulnerabilities earlier in the process can help to 'clean the slate' and provide a more stable base on which to build.

Deflating the Bubble

The IT industry is in a unique position. 'Softwarisation' is more than just a buzzword, and developers are building the future of every industry. As a result, few sectors would be insulated from the contagion effect of a global software-based attack. At a fundamental level, we need to keep in mind the power that software holds and understand the responsibilities that come with building it.

No one can accurately predict where, when or even if the security debt bubble will burst. The danger may seem remote, but it's only once a major incident has hit that the risks are truly appreciated. As an industry, we need to step up and put the checks and balances in place to reduce the risk as much as possible.

By repaying our debts now, we can safeguard the sector's health and gain the trust we need to build the future.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. It is our people that make us different.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

Orange
Cyberdefense

orange™