![TOOLS4EVER — IDENTITY GOVERNANCE & ADMINISTRATION]

IAM Whitepaper

FLEXIBLE MANAGEMENT OF IDENTITIES, USERS AND RIGHTS

Index

Introduction

The role of chief technology officer is evolving quickly because of the current spate of technology and its development. Not so long ago, CTOs focused heavily on IT operations and their organization's technology and design expansion. Now, much of their time is spent on business development and raising bottom lines.

The responsibilities of building the business and leading technology teams requires responsibility and broad shoulders. While their shoulders don't get wider, they continue to have responsibility thrust upon them, including everything from team development; leadership; technology; app development and design; and protecting the organization from outside (even insider) threats. It makes a CTO look at Atlas and think "if only I could be so lucky…"

Perhaps the most stressful factor facing most CTOs today is the unpredictability of people, both outside the organization and within. There's also the fact that five o'clock never seems to come. For CTOs, the work never stops - certainly not the work of mitigating threats to the organization. Constantly looming, breach paranoia keeps many CTOs up (literally) at night.

In addition to a lack of a good night's sleep, their mental health is at stake. The psychological toll of those in this profession can be enormous. Cyberattacks, tech outages and breaches cause stress-related illnesses and impact the mental well-being of 51% of tech executives, according to a survey of more than 850 C-suite executives from IT recovery firm Sungard AS. That number reaches 56% among CTO and CIO roles. To ensure their proper mental health, CTOs must ensure that systems are running smoothly – but there's more to this picture, as we'll see.

Digital disruption everywhere

No industry is currently spared from digital disruption – education, financial management, and even healthcare. Disruption creates a change moment that may seem particularly unwelcome to those forced to uproot their traditional ways of doing things. But disruption doesn't emerge from thin air. Disruption is caused by the capabilities of new technologies, the changing demands of customers or user, and the rapidly evolving practices of competitors. For example, healthcare is facing disruption because of consumer-centric organizations offering retail-like health and wellness services specifically designed to meet and exceed the expectations of today's healthcare consumers.

This disruption is front of mind for many CTOs who must adapt into more complex roles in the enterprise, which can give them plenty to be anxious about.

Asim Rais Siddiqui, CTO and co-founder of TekRevol, says the first thing he does each day, before even getting his morning coffee, is to make sure no disasters happened overnight. This line of thinking resonates among his colleagues: consensus shows that sleep may never be sound for CTOs. Each morning comes with the responsibility of ensuring everything, technologically, within the organization is still intact. Siddiqui is not necessarily referring to threats or cyberattack, but even keeping simple technology intact that makes the organization function.

"New technologies are unfolding all around us," Siddiqui said. "I believe every tech-based company is on some level vulnerable to new technology. However, the way out of this challenge is within our control. Our specific company culture encourages people to keep learning, stay up-to-date with the industry trends, and share their knowledge for the growth of the entire company."

Dealing with data management

Data management can be an unglamorous task: an arduous, technically challenging process that can drive decisions faced and made by organizational leadership. Even for tech leaders, the job remains difficult and often undesirable.

"Data management is updating package versions, it's documenting the process for who can access data and why, it's creating good access controls," said Vik Paruchuri, CEO and founder, Dataquest. io. "So, a lot of data [management and] security comes down to: Do you know who can access the data? Do you have procedures for who can access the data? And do you have the right patches and versions, the right versioning system in place for critical security updates?"

Burnout

While burnout may not receive the attention or credibility it deserves, the life of a CTO can be exceedingly stressful and filled with uncertainty. Some of this may be the result of the role being undefined without measurable expectations, a common occurrence because the role of CTO can be less easily understood than the roles of CFO or CMO, for example. Because of this, CTOs get pulled in many directions. This can result in their focusing less on their key areas of responsibility than other business priorities. This can lead to an identity crisis and being pulled apart by competing priorities – exacerbating burnout.

Andy Lipnitski, ICT department manager at ScienceSoft, agrees. The most challenging area of his work is managing the IT department – organizing IT operations, designing policies and procedures – while also considering the company's business objectives at the same time. "For this, I need to keep the perfect balance of working on the IT side and ensuring that the company's executives know the importance of IT improvements for the performance of their business."

Outside pressure

There's always outside environmental factors pressing upon any organization. "Keeping up with competition and the rate of change in the business environment today is a job in itself," said Stephanie Snaith, a director at Gradient Consulting. "Digital transformation is putting pressure on many companies to adopt new software and systems. Choosing to make a strategic change often shakes up an entire organization and can take months, even years, to settle down and until you see worthwhile results. By which time, the system is due another upgrade."

Likewise, Dan Fradenurgh, CTO at Strategic Real Estate Coach and Freeland Ventures, framed the most challenging aspect as staying ahead of what's taking place and not getting left behind by what's developing outside the organization. This includes what's coming up next and how these developments may impact the health of the organization long-term. By dropping the ball on monitoring outside influences, significant consequences are likely to occur.

A key aspect of leading an organization's technology effort is constantly learning new things. For example, technologies are advancing at such a fast clip that it remains vitally important to know when and where to invest in the next significant platform or disruption. Staying on top of every technological evolution can be overwhelming and time-consuming because they must decide when to commit to the trend and when to let it go. "It's very easy to be left behind if you stop learning what's out there," Fradenurgh said. That's not only dangerous for the organization but creates no small amount of toil for those approaching a decision.

Poor system design

A CTO's hands-on work starts with system design. Without solid design – and backing it up – even the best CTO is sunk. No matter how many strategies are tried, how agile an organization becomes, or how much DevOps are developed into the practices, none of it matters without coherent and functional design. Therefore, design is foundational to long-term success that platitudes and processes cannot make better on their own. Without quality design, improvement efforts have little effect overall and can create nightmare scenarios, especially where outdated technology is a factor.

Design functionality only goes so far, of course. Solutions that enable current design and infrastructure must be capable of supporting future integrations and developments. As businesses grow, they need to adapt to keep up with demand and need. Legacy systems are unlikely to cope with the speed of output required, and you will notice it becomes increasingly challenging to plan and manage resources, stock, orders, and materials.

"Without data-driven insight, it is impossible to make informed decisions," Snaith said. "As issues mount, the pressure extends from the system admin team to your employees; they are the people using the systems you have in place. In the modern-day, people expect easy-to-use tools to get their job done. If the systems you have in place are not fit for purpose, then something needs to change."

A CTO's biggest fear

According to Garth Wermter, CTO of Infranet Technologies Group, his second biggest worry is the insecurity of the non-business communication and collaboration tools used regularly: text messages, personal email accounts, shadow IT tools, and even BYOD. Inputs and outputs to systems can be secured, but time and again that humans conduct business through these personal devices, creating significant risk for the organization – leading to Wermter's biggest fear.

Despite fears about technology, most CTOs seem concerned about one thing above all: "My biggest worry is human mistakes," Wermter said. "We have great procedures that are well-documented, but our people still make mistakes – news articles show the business and financial impact of these errors daily. Our IT and security teams are not imaginative enough to predict and prepare our users for every threat variant."

It's difficult to outthink all the ways in which people can harm your organization. CTOs are very much akin to threat managers or watch groups protecting against attack. This is a yeoman's task make more difficult because they must lead their staff through skills gaps of various teams and business units. These gaps can hinder delivery and security, particularly as technologies evolve.

Even if gaps are not present, most CTOs know that the weakest link to the success of their initiatives remains the human elements. For example, the weakest link of any organization under a cyberattack is the staff. The mistakes that humans make allow attacks to succeed or spread further.

"The mindset of many in IT is still stuck in in the traditional perimeter, with firewalls and client VPNs," Andrew Moreland, CTO of Beyond M&A, said. "Often, their teams are blind to the larger security risks in their organization as a result."

According to a new study by Code42, 79% of information security leaders believe that employees are an effective frontline of defence against data breaches even though facts seem to counter this claim. Some organizations have not put in appropriate detection and response data security controls and, instead, trust employees to keep data safe. The study shows that employees take more risks with data than employers think, which leaves organizations open to negligence and insider threats. In most breach cases, human error is the culprit.

Likewise, as for the technologies adopted, they need to be intuitive and easy to use for the people using them. Technologies that are difficult to adopt encourage people to turn towards workarounds that may create an unmonitored attack vectors.

Do the basics right

"As long as you keep your technologies and systems on the latest version and latest patch, you can protect your system very well. Hence, before you go to more sophisticated stuff, make sure to get the hygiene right first," Siddiqui added.

Getting the basics right can be anything but basic. As discussed here, the role of CTO is evolving and continues to do so. So, getting even the most basic function correct – like security and threat protection – is more complicated than many may believe. The basics for a CTO today are vastly different than they were just a few years ago. For one, CTOs' primary role is on business development rather than on building out IT infrastructure. As such, these leaders often experience overwhelming responsibility for how the organization performs as well as what it can perform.

There's quite a bit that keeps CTO up at night. If the basics aren't done right, all that may remain are nightmares.

Contact us

There are a lot of disruptions and responsibilities on a typical CTO's plate. Tools4ever offers a suite of solutions that can alleviate any potential pain point a CTO may have, removing concerns on possible back-end infrastructure issues, or other problems that can arise in daily operations. With Tools4ever, CTOs are finally able to focus on the priorities that matter.

If you would like more information on the subject of IDM solutions or to set up a consultative discussion with Tools4ever regarding steps to improve your organization's IT administration, please contact one of our North American offices (listed below).

For more reading on Tools4ever's IDM solutions and consultative expertise, please visit: tools4ever.com/resources/ or tools4ever.com/references/

Tools4ever's complete range of IDM solutions includes:

✓ Identity and Access Manager (IAM)

✓ HelloID (Cloud-Based IDaaS & SSO)

✓ Self-Service Reset Password Manager (SSRPM)

✓ Enterprise Resource Authorization Manager (ERAM)

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER New York		TOOLS4EVER Washington	
Address	300 Merrick Road, Suite 310 Lynbrook NY 11563 USA	Address	11515 Canyon Road E Puyallup WA 98373 USA
Phone	1-866-482-4414	Phone	1-888-770-4242
Website	tools4ever.com	Website	tools4ever.com
Info	nainfo@tools4ever.com	Info	nwsales@tools4ever.com
Sales	nasales@tools4ever.com	Sales	nwsales@tools4ever.com