The 12 biggest issues IT faces today

From securing IoT to retraining IT talent to finding new revenue streams, CIOs have more than their share of concerns keeping them up at night.

By Paul Heltzel
CIO | JAN 8, 2018 3:00 AM PT

When CIOs aren't being overwhelmed by data, they're wondering who's securing it. They're dealing with the pressure of cutting costs while trying to stay nimble as they face difficulties with contractors and the challenges of moving data and services to the cloud. All the while, new threats emerge that require an evolving response.

From finding qualified IT pros to keeping them from jumping ship, a range of sticky technology and personnel issues are giving IT pros cold sweats.

With a host of new concerns in 2018 — and old standbys — where should CIOs be most focused? We've gathered insights from experts, the C-suite, recruiters, and those in the trenches to identify today's top-of-mind concerns and how to deal with them.

[Beware the 12 'best practices' IT should avoid at all costs while coming to grips with the 6 hard truths IT must learn to accept. | Get an inside look at 10 real-world digital transformations. | Get the latest insights by signing up for our CIO daily newsletter.]

IoT security

A recent Forrester security study found that 82 percent of organizations struggle to identify and secure network-connected devices. Worse, most were unclear on who is responsible for managing the devices.

“Survey results show that over half of the respondents (54%) stated that they have anxiety due to IoT security,” the study reported.

Csaba Krasznay, security evangelist at Balabit, says that, along with traditional weak links (read: users), CIOs need to be thinking about new emerging threats.

“In 2018, security measures should be more closely aligned with IT users and their identity, Krasznay says. “Behavioral monitoring can detect even the smartest cyber criminals lurking behind privileged credentials, by discerning deviations in baseline behaviors — even based on minute biometric traits such as typing speed or common spelling errors.”

Retraining

About 40 percent of IT workers say they’re not getting the training they need to be effective in their jobs, according to a recent CompTIA survey.

“Many companies believe that keeping up with technology is the responsibility of the individual employee,” says Viktor Andonov of DataArt Bulgaria. “That might have been true in the ’80s and ’90s, but in the 21st century, the complexity of platforms grew enormously. Training on the job and learning how to work with new frameworks is extremely difficult when employees have projects and deliverables too.”

Most organizations struggle with finding qualified tech staff, says Todd Thibodeaux, president and CEO of CompTIA. Training them up on the clock feels equally daunting.

“The good news for employers is that the majority of IT pros like what they’re doing,” Thibodeaux says. “Their jobs provide them with a sense of personal accomplishment. Their skills and talents are put to good use. They see opportunities to grow and develop in their careers — and they’re generally satisfied with their compensation and benefits.”

While IT staff may enjoy their work, retraining goes a long way in keeping it that way, says Thibodeaux.

“IT pros would like more resources for training and development, and more career path guidance and career advancement opportunities,” he says. “They’re also interested in having access to more tools and engaging with more technologies and applications. And they’d welcome the opportunity to work on new technology initiatives.”

It’s not a new problem for 2017, Thibodeaux says, but it’s an ongoing one. “After all, time set aside for staff training is time taken away from billable hours or ‘real work.’ There’s also the age-old question, ‘What if I train and certify someone and they leave?’ But when it comes to technology and the people they’re paying to implement it, the question they should be asking is, ‘What if I don’t train someone and they stay?’”

Data overload

Current methods for analyzing data frequently fail to show the real impact on business, says Mike Sanchez, CISO of United Data Technologies.

“Executives and board members should be able to make decisions on how best to allocate resources, and investment dollars into remediation strategies that can reduce operational expenses, or a company’s true risk exposure or both,” Sanchez says. “There’s too much data out there and folks don’t know which they should be following in terms of improving their overall cybersecurity posture. Key performance metrics should tell the story in a simple dashboard format.”

Skills gap

The good news is the number of IT job openings continues to increase. The bad? There aren’t enough workers with needed skills to fill them, particularly in security roles.

“Our latest analysis of jobs data from a variety of sources shows that in Q3 2017, U.S. employers posted openings for nearly 604,000 IT jobs,” says CompTIA’s Thibodeaux. “Regarding cybersecurity jobs, we’ve made some incremental progress in closing the gap over the past year, but not nearly as much as needs to be done.”

Thibodeaux says firms are going to have to make some hard decisions over how to fill staffing needs and what needs to be done in-house.

“Which functions might be candidates for outsourcing to a technology solution provider?” Thibodeaux says. “Many organizations find that contracting with a technology partner for some routine, ongoing tasks can free up internal tech teams to focus on activities that are more advanced and strategic to the business.”

Meerah Rajavel, CIO of cybersecurity firm Forcepoint, says the skills gap isn’t going away anytime soon.

“We see too many companies are unprepared to deal with new cybersecurity threats like ransomware or industrial espionage,” Rajavel says. “Any course correction needs to include appropriate talent grooming from the bottom up, and broader workforce security training which should be experiential and just-in-time rather than just compliance.”

Innovation and digital transformation

According to Gartner data, about two-thirds of business leaders think their companies need to speed up their digital transformation or face losing ground to competitors.

Most companies will continue on the same path until they’re forced to do otherwise, says Merrick Olives, managing partner at cloud consulting firm Candid Partners.

“Tying IT spend to strategic business capabilities and answering the question ‘How will this make us more competitive?’ is essential,” Olives says. “Value stream-based

funding models as opposed to project-based funding are becoming more and more effective at tying board-level objectives to budgetary influences. The cost structures and process efficiencies of legacy vs. a nimble digital capability are much different — nimble is less expensive and much more efficient."

Tightening budgets

Along with skepticism from higher-ups, nearly half of IT and line-of-business respondents said that budgets were a barrier to firming up IoT security, according to a November 2017 report from Forester.

CompTIA's Thibodeaux says the risks go beyond security threats.

"It comes down to the question of whether the business wants to grow and thrive or get left behind by their competitors," Thibodeaux says. "As businesses become more digital, technology moves out of the background shadows to center stage where it becomes the primary driver to meet long-term objectives. Skilled, trained and certified IT professionals are essential to make investments in technology pay off. They have the expertise to connecting and IT architecture to the overall corporate objectives and can provide the guidance decision-makers need to evaluate the tradeoffs involved when selecting devices, applications, or operational models."

Finding new revenue streams

Ian Murray, vice president of telecom expense management software firm Tangoe, says that while the business landscape is ever evolving, the basic premise of making a profit is the same.

"The process to finding and exploiting revenue opportunities hasn't fundamentally changed — find a problem that we can solve that is common, prevalent and that people will pay to solve," Murray says.

What has changed is the emphasis on direct revenue generation landing in the CIO's lap, says Mike Fuhrman, chief product officer of hybrid IT infrastructure provider Peak 10 + ViaWest.

"Maybe I'm old school, but I don't think the CIO should be worried about directly generating revenue," Fuhrman says. "I'm starting to see this pop up more and more among my peers. To stay relevant as a CIO, many are working to try and productize themselves. While there are benefits to thinking that way, I think it can also be a recipe for defocusing the team and the boardroom. When it comes to revenue-generating opportunities, the place the CIO belongs is focusing on those projects and digitizing the business into an automated platform at scale. We need to stay focused on driving costs out of the business and scaling from a go-to-market perspective. That's how a CIO should focus on revenue."

Upgrading legacy systems

Staffing firm Robert Half this summer created a report that found nearly a quarter of CIOs were most concerned with upgrading legacy systems to improve efficiency.

“This is a big concern particularly among several industries where a large number of outdated or end-of-life systems are still being used to hold mission-critical data or applications,” says United Data Technologies’ Sanchez. “These systems are no longer supported by their respective manufacturers and therefore can no longer be patched with the latest version of upgrades leaving these systems vulnerable to exploits. These platforms can be interconnected to other networks which allows vulnerabilities to extend outward and include those interconnected systems in attacks.”

Lack of agility

Organizations that aim to incorporate agile methods sometimes end up limping along in a sort of hybrid model that incorporates agile practices but also more linear “waterfall” methods. In short, the worst of both worlds.

Tangoe’s Murray lays it out: “Developers are coding to specific spec sheets with little conceptual understanding of how this button or feature fits within the overall user experience. A disciplined approach is needed to pull this off, where the solution to specific problems are addressed within a certain release. Each release is then coordinated for a set of sprints so that a comprehensive solution that adds to the UX is achieved with every release and not just a collection of requested features that may or may not support one another.”

Murray points to recent Apple iOS updates, which fixed some bugs and introduced others. “This problem affects companies large and small,” Murray says, leading to updates that may address security flaws and include new features, but also create well-publicized headaches for users.

Outsourcing risks

The skills gap will lead many organizations to seek outside help. But these sometimes-necessary solutions can lead to concerns with reliability and security.

“Our main focus is to deliver on the promises we make to each customer,” says Sanchez. “You build your reputation and business on this one critical thing. In outsourcing your work, the quality of the deliverable is sometimes at the mercy of the firm you outsourced to. Given the sensitive nature of the projects we manage, we utilize strict third-party vendor assessments to evaluate partners in the event a project requires us to consider outsourcing some or all of the required tasks.”

In addition to quality concerns, outsourcing opens up security threats that are well known. “The specific threats for CIOs that should be top of mind are the insider and the contractor,” says French Caldwell, chief evangelist with MetricStream and a former White House cybersecurity advisor. “Until we move away from passwords for credentials, humans will continue to be the biggest threat.”

Pitfalls in moving to the cloud

As more data and services are offloaded to the cloud, a potential risk is viewing the cloud as a single, public entity, says Bask Iyer, CIO of VMware and Dell.

“IT needs to also look at a private cloud and/or multi-cloud solutions as they evaluate what’s best for the business,” Iyer says. “This ensures choice and avoids single-vendor lock-in. IT also needs to ascertain which apps should go to which cloud. With the rise of IoT, more horsepower is needed at the edge so IT needs to expand their options for the cloud.”

And CIOs can’t transfer the responsibility of securing their data and apps to the hosting company, says Sanchez. “Organizations must define security controls to safeguard their data in the cloud in much the same manner as it would when it’s on their site. Many organizations don’t apply these standards and automatically assume the hosting company is providing all of the safeguards they require.”

Multiple security vulnerabilities

According to Larry Lunetta, vice president of Hewlett-Packard's Aruba unit, security nightmares will continue this year, and the top worry is hiding in plain sight.

“Future headline-making exploits will co-opt legitimate credentials as the starting point for an attack that can take days, weeks or even months to begin and finally do damage,” Lunetta says. “These attacks on the inside can begin with a user clicking on the wrong email attachment, a disgruntled employee going rogue, or as the result of weak passwords or sharing of credentials among colleagues.”

New behavioral-based detection techniques will be needed in 2018 to address the threats, says Lunetta.

“Increasingly, organizations are using artificial intelligence-based, machine learning User and Entity Behavior Analytics systems to spot small changes in behavior for users and network-connected devices that are often indicative of a gestating attack.”

Original article: https://www.cio.com/article/3245772/it-strategy/the-12-biggest-issues-it-faces-today.html