Industry Panel unearths Shadow IT challenges, solutions

Participating CIOs acknowledge that taking a more collaborative approach to IT with business users can help to turn the threat of Shadow IT into a business or competitive advantage.

Shadow IT, a largely derogatory term that gets IT departments up in arms, is often a product of failed opportunities.

Telstra's report entitled "Rise of the Superuser", a global survey of 675 IT decision makers in Australia, Hong Kong, Singapore, the UK and the US, showed that shadow IT is rampant — despite systems, processes and policies to contain it. The survey revealed that nine out of 10 IT leaders struggle to deploy the communication and collaboration tools IT really wanted. Often this need is driven by productivity.

In the past, if IT did not implement a certain tool, the employee would have very little opportunity to deploy it within the enterprise infrastructure.

"Traditionally, we were all about getting the right hardware and software, deploying them at minimal cost and making sure it kept working. Now, businesses are saying that if my IT department does not give me what my business needs, we will go external," said Chris Mohan, General Manager, Security Controls, Telstra, who noted that it is now simple to buy entire server farms or subscribe to applications that can be accessed on any device.

This creates a security vacuum. "You know these technologies exist, but the policies and processes to protect your data are not. That means the data, the lifeblood of businesses, is no longer under your control. In an environment where shadow IT exists, the focus on security is absolutely critical," said Mohan.

Mohan believes that instead of fighting against users, it may be time for businesses to take a step back and develop a simple risk framework. With businesses and decision makers used to dealing and managing business risk, it offers a starting point to tackle the risks that Shadow IT introduces.

> ***"You need to embrace Shadow IT. Taking a partnership approach [with your business users], applying risk and security policies, and collaborate. It is the only way an organization is going to succeed"***
>
> ***– Sundi Balu, CIO, Global Enterprise & Services, Telstra***

"Essentially, it allows them to take the appropriate measures to handle these risks," he said.

Such a framework will let you know the value of the data, who accesses it, where it is stored, know who is protecting it and how well it is protected. "These are really good starting points for managing shadow IT," he added.

Stop restricting, start engaging

With such a framework, what can Hong Kong organizations do next to combat Shadow IT?

That was the main question that was asked to four leading senior executives participating in the Computerworld Hong Kong Executive Panel Discussion entitled "Shining through the digital era with shadow IT".

According to the panelists, it is time to embrace Shadow IT. "You need to embrace Shadow IT. Taking a partnership approach [with your business users], applying risk and security policies, and collaborate. It is the only way an organization is going to succeed," said Sundi Balu, CIO, Global Enterprise & Services, Telstra.

The rise of Shadow IT also highlights the strained communications with the business users. "I think it is all about IT communicating with business. If people do not trust IT, or IT is not aware of the business requirements, then things can go wrong. I think you need constant dialogue. At least then you can advise them," said Andrew Koh Meng Wee, Deputy Chief Manager, Risk Control, China Construction Bank (Singapore).

The opinions echoed the conclusions of the Telstra report. It highlighted that the principal roadblock to adopting employees' preferred IT was not ignorance, but the reality that other IT goals take precedence. Forty-seven per cent of respondents claimed that having higher priority IT projects prevented them implementing the technologies that end-users wanted.

Not all industries, companies are the same

Although panelists agreed that IT needs to get closer to business, the approach will vary according to the business and industry.

"I think it depends on what industry and company you work in. If you are in an industry where there are not many strong regulations or people do not work with sensitive customer information, then IT having central control may not be the best approach. Maybe having IT be driven by business user needs

may be better. But in my company I do not see that happening. We have a lot of sensitive customer information and a lot of regulations, and regulators have a high expectation on how we protect customer data," said Henk ten Bos, Chief Information Officer, Ageas Hong Kong.

"The moment you let people go to the browser, it becomes very difficult to control. You can block access to certain websites, but we can't forget that they have the mobile phone that easily can overcome that. So we work on a policy of self-declaration. We rather let each employee to declare," added Koh, describing his company's approach to managing Shadow IT.

Balu pointed out that data has become the new currency. "It's like oil. So to manage it, you need to have a perspective on what are your critical assets, threats and vulnerabilities. It's like a Venn diagram and it is the intersection point that you need to care about," he said.

It's a delicate balancing act

While panelists debated the merits of increasing education and engagement with end users, they agreed that IT leaders need to forgo the notion of 100% security.

"You will never live in a world where you can secure your data 100% because of the prevalent nature of connectivity and accessibility. What you need to do is to identify and classify your data and look at the vulnerabilities against that data and associated threats. Once you have that knowledge, you can put a lot of controls," said Balu, who argued that IT departments need to stop controlling, and start collaborating.

According to Koh, IT needs to start managing risks. "Yes, there will always be risks out there. You can never detect it all no matter how many tools and processes you have. But once something occurs, you need to have the right contingency plans to manage this. For this to happen, you need to have the right thought process, while constantly revising your policies," he added.

Balu pointed to machine learning as another approach that is helping companies tackle the risks of Shadow IT.

"There is very interesting stuff there. It is managing chaos, to discern patterns in chaos and learn in quantum velocity. If there is a human behavior that can be quantified, then it can be detected, and then when the deviation occurs, you can take proactive action. It is similar to your body, where your immune system may not know all the pathogen it will attack but knows enough to detect variables," he added.

It is a delicate balancing act that needs to begin today.

"I think you need to find a balance between your IT needs and the users. So that they can be productive, balanced by the proper policies and guidelines. If you work in a corporate environment you need to accept that you need to adhere to corporate policies and standards. But these need to be flexible enough and tools be good enough so people do not have to think about going to Shadow IT," said ten Bos.