[article title]

Coming Out of the Shadows

[subtitle]

Getting on Top of Applications Managed by Teams Across the Business

[byline]

By Renee Tarun
Vice President Information Security, Fortinet

[body copy]

An employee needs finish up some work on a Word document after the kids go to bed one evening, so he saves the file to his personal Dropbox account. A marketing team is working with an agency on a specific go-to-market initiative and creates a free Slack account to help with collaboration. A manager contacts her direct reports after hours using WhatsApp or Snapchat, figuring the employees will be more likely to notice the message. A DevOps team, facing constant pressure to meet its time-to-market goals, sometimes uses third-party code from unvetted sources. A business unit whose products and customer base are distinct from the rest of the company finds that the corporate CRM does not meet its needs, and deploys a cloud-based alternative for its small sales force.

These are examples of company workflows being performed on IT systems outside the control—and often the knowledge—of the IT department and the CISO. This practice has historically been referred to by the sinister term "shadow IT"—and that description is not inaccurate. All too often, the CISO only finds out about a shadow IT application when something goes terribly wrong.

I do not need to waste time convincing you that this scenario is a real problem and poses real risk to your organization. Instead, what I want to address here is how to manage this situation in such a way that you can gain visibility into existing Shadow IT apps—and earn enough trust around the organization that business units are transparent with you about new services they want to deploy.

Why Do People Use Unauthorized Applications?

I want to start with a few observations about the typical motivations behind Shadow IT:

- Practitioners of Shadow IT often have no ulterior motives but are simply wanting to find ways to do their jobs more efficiently and effectively.
- Many perceive that going through an approval process for a new service will slow things down significantly. Worse yet, some think the IT or cybersecurity departments are "where innovative ideas go to die."
- Many assume that the CIO or CISO would simply shut down their applications if they found out about them—which motivates users to keep them secret.
- In some cases, employees are so accustomed to seamlessly using multiple apps in their personal lives that it does not even occur to them to consult IT before using them for work.

In short, the people who deploy these apps usually do not intend to bring harm to the company. But as I often say to companies I am consulting with, one definition of an insider threat is "good intentions with poor implementation."

The Hard Work of Changing Perceptions

I want to point out how much these perspectives are based on perceptions that can be changed. It will take intentional effort and relationship building on the part of the CISO and CIO, but it is truly possible to transform the above scenarios to the following ones:

- Through improved lines of communication, those who just want to do their jobs more effectively might learn that an enterprise application already exists that does what they need.
- Through ongoing communications and collaboration, employees can find the process of adding new applications to be collaborative and streamlined—with a focus on meeting business needs in a timely manner.
- During an "amnesty period," employees could be encouraged to come forward with all applications in use—not to shut them down, but to integrate them seamlessly and securely. The paradigm can then move from "allow or deny" to "manage and monitor."
- Through ongoing positive contact between the IT and cybersecurity teams and the various business units, employees might remember (and care about) the risks that third-party, consumer-focused apps pose to the company.

From Shadow IT to Business-managed IT

While Shadow IT has been discussed for many years, a less pejorative moniker, "business-managed IT," has been trending recently. And while the term is sometimes used to describe practices that are not all that different from Shadow IT, I believe the terminology can give us some guidance on moving forward.

According to the Harvey Nash/KPMG CIO Survey 2019, 43% of enterprises report that more than one-tenth of their technology spend is now managed outside the IT department. Business-managed IT is still completely prohibited at 36% of organizations surveyed. But that means that nearly two-thirds of organizations now allow it, and 11% actually encourage it. According to the report, many organizations now see business-managed IT as "a useful tool for empowering the business, removing bureaucracy, and getting closer to the customer."

The report found that in general, organizations that encourage business-managed IT are much more likely to out-score their competitors in a variety of areas—including customer experience, employee experience, and time to market for new products.

Security: Key to the Success of Business-managed IT

But of course there is a catch. The same research shows that business units that deploy services *without* consulting the IT and cybersecurity teams are twice as likely to have exposed the company to security issues in multiple areas and 23% less likely to have effectively built customer trust with their technology.

These results indicate what you probably already knew: If done in collaboration with the CISO and CIO, business-managed IT can propel the business in many ways. But if these departments go off and do their own thing, security issues can negate any positive benefits that might have been realized.

From the CISO's perspective, it really does not matter who is managing a service as long as it is visible to the SOC team and does not add to the company's risk. Ideally, every business-managed service will be a part of the integrated security architecture so that your team has full visibility and control and policies are managed consistently.

A Collaborative Model for Business-managed IT

So how do we get from here to there? The short answer is that it takes a lot of relationship building—with other executives, with the board, and with rank-and-file employees. Here are a few suggestions that I have gleaned as I meet with CISOs in many different industries:

- *Do what it takes to understand the needs of your business.* This requires networking and communication. If you do not currently meet at least quarterly with every business unit leader, you should start doing so.
- *Find ways to "translate" risk for different audiences.* When it comes to communicating IT risk to other parts of the business, it is all too easy to be *way* too technical. CISOs need to develop skills in portraying that risk in business terms that the board and CEO can understand—and in personal terms that rank-and-file employees can identify with.
- *Work closely with vendor management and procurement teams.* If someone from your team is not a part of the vendor certification process, that needs to change immediately. Each vendor's cybersecurity posture should be reviewed at least annually, and every vendor contract needs to have a security addendum. New technology vendors should be required to fix security issues in their products before deployment.
- *Be careful with APIs.* Business-managed apps will inevitably need to be integrated with your ERP, CRM, HRIS, or other systems. Make sure the security of vendor APIs is certified before exposing critical company data to increased risk.
- *Make sure that business-managed IT is not really "unmanaged IT."* Business leaders who do not know much about IT assume that SaaS applications "run themselves" and do not need much management. "Joe Smith knows all about that app, so we're covered," they might say. But what if Joe Smith goes on vacation—or worse yet, leaves the company? CISOs should insist on a *real* management team and succession plan for business-managed apps.
- Speaking of management, *make sure business units maintain patches* for their applications. As I wrote in Phil Quade's book, *The Digital Big Bang*, not doing so is like leaving the doors unlocked for a thief who wants to break into your house.
- *Focus on standardization.* Standardization of networking and security systems is very important for compliance, and shadow IT applications can introduce unknown data flows that put compliance at risk. Integration is key, and achieving it probably requires a lot of collaboration.

That is a long list of suggestions, and at one level it may seem overwhelming. But it really boils down to a relatively sumple principle: *build a collaborative culture of security.* It is impossible to "put the genie back in the bottle" when it comes to business-managed IT—and research shows that we may not want to anyway. But we can be deliberate about cultivating innovation to propel the business—without increasing risk. It is truly possible to move from shadow IT to business-managed IT.