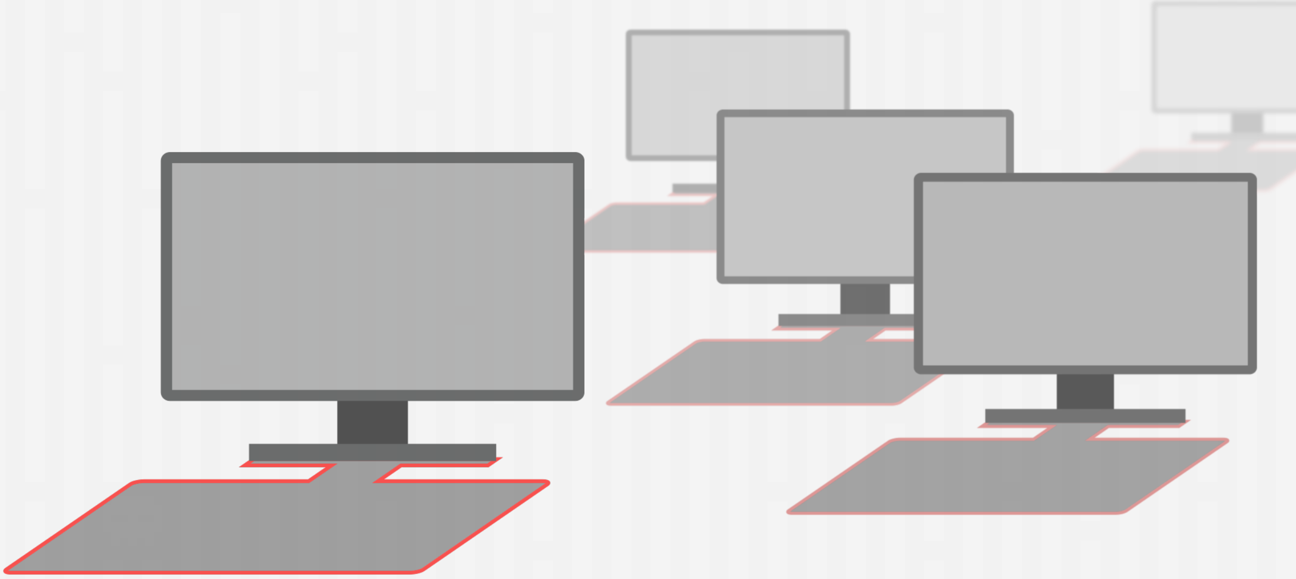
CYBERSPRINT
BREAKTHROUGH SECURITY

EDITORIAL

6 STEPS TO ACHIEVING ZERO SHADOW IT



BY PIETER JANSEN
CEO CYBERSPRINT

6 STEPS
TO ACHIEVING ZERO SHADOW IT

BY PIETER JANSEN
CEO CYBERSPRINT

Shadow IT has long been a problem for organisations. Formal IT is routed through the IT department, where it's approved, purchased, set up, and, importantly, supported and maintained.

Shadow IT falls outside this process, and is normally split into two categories:

- Systems that the IT department doesn't know about.
- Systems the IT department knows about but needs to keep running as they are integral to business operations.

The second category is the real Shadow IT and the biggest problem for businesses.

There is a reason we have formal processes for acquiring and setting up IT infrastructure and software. It's so the company knows what software and infrastructure it is operating and that any risk to the business is being appropriately managed. I can tell from experience that things falling outside this scope could represent a serious source of uncontracted third-party risk.

The knock-on effect of this process means that it can take time to get things set up if you go through the formal channels. One thing that most Shadow IT systems have in common is that they are typically quick and cheap to set up — falling below the limits of credit card spend, so there is no procurement involved — and they invariably fulfil a rapid need.

> “ONE THING THAT MOST SHADOW IT SYSTEMS HAVE IN COMMON IS THAT THEY ARE TYPICALLY QUICK AND CHEAP TO SET UP”

While this may all start innocently, it can end badly. We recently uncovered a situation where a department had set up an online questionnaire, which had been included in newsletter to customers. They'd used a free version of the software and it had not been authorised by IT. The questionnaire requested some quite sensitive data, but as there was no third-party contractor agreement in place, there was no agreement on data usage, storage, protection or maintenance. As it turned out the software provider had a security vulnerability in their solution, and this resulted in a massive data breach of the questionnaire answers.

So how can you protect your business from the perils of shadow IT? Here are my six steps:

1. DON'T FIGHT IT, EMBRACE IT

Shadow IT is created for a reason, mainly because people have a need to implement a system (perhaps a website, a testing environment or a survey platform), and they need to have it up and running quickly. They don't go to the internal IT department because they know that takes time. But it takes time for a reason. IT applies security, they apply hardening. They do all the checks that need to be done in order to have a secure piece of technology that is not going to cause the business problems down the line. The first step to tackling shadow is not to fight it but to embrace it. To understand there is a genuine need for these systems and look at how you can accommodate them into your framework.

2. CREATE A FAST TRACK

One of the first things we ask our clients when looking at Shadow IT is, “do you have a fast track?” Having a process in place that enables departments to push through system deployment as quickly as possible means they are less likely to bypass IT, as they are no longer seen as a roadblock to deployment. Instead, they are seen as an enabler. This may mean having pre-agreed relationships with a handful of key suppliers to handle online and infrastructure assets, but however it works it’s a key step in bringing IT out of the shadows when people want something done fast.

3. COMMUNICATE EFFECTIVELY INTERNALLY

Of course, there’s no point in having a fast-track system in place if people don’t know about it. Employees need to know and understand the role of IT in this process, and how they can push their systems requests through if they need to. Practically, this means they need to know where the forms are to get something done quickly. They also need to understand why doing things outside of the IT department can present a serious risk to the organisation, and this may require an element of education.

4. TAKE OWNERSHIP

This is great for moving forward, but what about systems that are already in place. How can you protect against things that you don’t know exist? For physical things like IoT devices it might be relatively easy to locate them on the network, but doing so for hidden systems and software is much more complex. Not to mention Shadow Cloud. Preventing data leaks is something that should be done as group, so creating an amnesty programme for shadow IT is a great way to bring things into the open. Ask teams to report any shadow IT they think they may have without fear of reprisal. Once ownership has been established you can work out whether the systems in question are still needed. If so, bring them under management. If not, determine whether they can be switched off.

Related to this topic is the type of experimental IT that needs to be tested, but cannot be completely facilitated according to official governance policies. Examples are the testing of a new dataset or innovative technique. Even though it does not follow standard procedures, it’s important to be aware of such things to set up monitoring for controlled IT experiments.

5. CREATE MIGRATION STRATEGIES

For systems that are business critical, it may be necessary to migrate them onto other platforms that are under preferred suppliers. This is going to take planning, from negotiating contracts to actually managing the migration to new platforms. Whatever the situation, IT will need to make plans to integrate these systems into their management structure and then manage that transition with the least impact to the business.

6. PREPARE FOR THE FACT YOU MAY NOT BE ABLE TO TURN IT OFF

There will be systems that are critical to the business but for whatever reason it's not possible to migrate them to new platforms. At least you know about them and can put monitoring processes in place. In practical terms this means ring fencing the core of these systems so that they present as little risk as possible to the organisation. If these are physical devices, such as IoT, you may be able to deploy firewalls or data filtering to ensure they are not being compromised. If at some point in the future they can be decommissioned or shifted then great, but at least in the meantime you know they exist.

> Ultimately, I believe creating a zero shadow IT environment is about empowering the IT department. Empowering them to be enablers. The IT department needs to be seen as a friend by the rest of the company, a friend that can get whatever systems they want up and running as quickly as possible. Because from IT's perspective, if something is in their configuration management database, it's no longer shadow IT.

ABOUT THE AUTHOR

PIETER JANSEN is a passionate cybersecurity specialist and CEO & founder of Cybersprint. With his experience as an ethical hacker and security manager, Pieter has worked on both the 'offense' and 'defense' side of cybersecurity. Pieter saw new possibilities in developing a platform to automatically map the attack surface of organisations. He started his own company, driven by his ambition to make the digital world more secure. His motto "Defense is hard, offense is easy" forms the base of the Cybersprint platform.

ABOUT CYBERSPRINT

Cybersprint maps the attack surface of organisations and brands. We offer full visibility using continuous and automated digital asset discovery. Our zero-scope approach provides an outside-in perspective, eliminating blind spots.

Assets are individually scanned for a multitude of risk types. These insights empower cybersecurity professionals to prioritise the mitigation of vulnerabilities. Our integrated AI correlates dozens of data sources and uses a multitude of scanners, making risk relevant.

Cybersprint's SaaS platform allows organisations to manage and monitor risks with customisable filters and alerts, integrated into existing processes. Detect and prevent threats such as phishing, brand abuse, data theft and more.

Visit www.cybersprint.com