IT'S CALLED SHADOW IT FOR A REASON

BY JAY BORDEN

Let's start by defining shadow IT. IBM defines it this way:
"Shadow IT is any software, hardware or information technology (IT) resource used on an enterprise network without the IT department's approval, knowledge or oversight."

A very broad definition but accurate. Shadow IT has existed for a long time. However, introduction of Software as a Service, SaaS, and cloud service models accelerated it. Now AI is speeding it up even more.

Why does shadow IT exist? Basically, because the business needs to move quickly to stay ahead of competition while IT moves more slowly to properly investigate and secure all IT assets and company information.

Both the business and IT have valid arguments. The business tends to win because they bring in the money. IT is often viewed as a roadblock or delayer.

IT assets or services acquired by the business come with high risks to the company. SaaS and AI are adding to the risks yet making acquisition simpler and more tempting.

Despite knowing the risks, research found almost 75% of those surveyed admitted using a SaaS service that is unknown or unauthorized by IT.

The risk keeps growing because cybercriminals are becoming more adept.

Cloud systems and SaaS have been sold as putting the operational burden on the vendor. All people need do is use it. Sounds good but not true. Even cloud systems overseen by IT have been compromised due to the complexity of keeping them secure and lack of clarity about who is responsible for securing the different parts of it. This has resulted in a number of recent breaches.

Copyright 2020-2023 OneBrightlyCyber,Inc.

IT'S CALLED SHADOW IT FOR A REASON

CONTINUED

AI systems add additional risks. In many instances people entered confidential information into an AI system to get what they needed. The response from the AI system may have been satisfactory, but what happens to the confidential information given as input? Is it used by the AI system for any other purpose? Is it maintained by the AI system and at risk if the AI system is compromised?

AI system risks are well documented as far as they are known. But the big problem is that the exact behavior of these systems is not known. All the AI systems hallucinate, that is, give answers completely unsubstantiated by facts or evidence. No one knows why they do it, so how can it be stopped?

Cybersecurity is very complex with attacks continually changing. Attackers keep finding new ways to compromise things and steal information and install malware. SaaS systems are targets due to the information from various companies contained on the system.

Even with a fully staffed and skilled IT team, protecting assets is not easy as evidenced by the number of breaches that occur.

What can be done?

Keep all assets up to date with the latest versions of the operating system and the applications.

If an asset, hardware or software has reached end of life, meaning it is no longer updated or supported by the manufacturer or developer, replace it as soon as possible. Holding things beyond that point introduces significant risk. Attackers know the security weaknesses and work to exploit them.

What about all the hardware and software and services that aren't end of life? Any IT asset acquired and managed by the business has probably not been investigated as to its cybersecurity or had proper controls put in place.

Copyright 2020-2023 OneBrightlyCyber,Inc.

NOT REALLY TECH SUPPORT

CONTINUED

Accepting that the business will continue to have Shadow IT, we recommend that IT at least be informed about all assets acquired by the business. That way they can maintain an up to date inventory of what is connected to the network and any cloud and SaaS systems being used. IT may be willing to maintain the systems and keep them up to date.

IT may be able to vet vendors offering the type of systems being considered by the business and suggest one or two that are considered the most secure.

This is not as secure as vetting everything first, but it is a step forward.

As we said at the beginning of this Insight the business has a valid need to move quickly. It is up to the executives and the Board of Directors to stay on top of this and balance the needs of the business with the risks incurred by Shadow IT.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.

Copyright 2020-2023 OneBrightlyCyber,Inc.