INSIGHTS

Cyber made simple.

one brightly cyber

SHADOW IT INCREASES CYBER RISKS

BY JAY BORDEN

We have written before about the risks of shadow IT, which is defined as computers, servers, applications, even cloud based applications, or any other related things that are chosen, acquired, used and managed outside of IT's domain and control.

The challenge is that these applications and services may not be properly secured or that users may be given more access than is wise according to Zero trust or minimal privilege approaches.

Business groups typically look at the business value of a service or application and how quickly it can be implemented. This is understandable given their role. They are less familiar and concerned with regulatory requirements and how to protect information.

If there is a breach or information is stolen, regulators will look at how the information was protected. If it is determined the company is out of compliance or did not properly secure protected information they can impose significant fines.

Cyber insurers may well deny claims. And your reputation will be negatively affected when it comes out that that you failed to take care of Personally Identifiable Information, PII, and Non-Public Information, NPI, of customers or employees.

These concerns are not idle unfounded thoughts on my part.

A recent research report by Ponemon Sullivan, a highly regarded source, found that companies are unaware of how many applications exist outside of the knowledge and protection of IT or an identity management service that has been vetted and meets industry standards.

SHADOW IT INCREASES CYBER RISKS

Continued

Only 49% of companies surveyed even track applications that exist outside the knowledge of IT. Of those that do track them , only 21% rated themselves as highly confident their tracking is accurate.

The research finds there are on average 96 applications outside of IT control. Almost one quarter, 23%, of surveyed companies have between 101-250 applications in this category. That is a great deal of unprotected information!

Now it is important to remember that these counts are what is known and cannot account for what is unknown. With only 21% of those surveyed highly confident of their tracking, the actual number may be far higher.

Of those participating in the survey, 52% reported a cybersecurity incident due to applications outside of IT control.

A full 54% of respondents acknowledge that granting or revoking access to the non-IT controlled applications is in the hands of the business units.

Failing to use proper identity management means passwords do not have to meet certain requirements and can be reused further jeopardizing information security and the company.

Companies understand that the risk is due to these applications not using industry standard identity and security standards or meeting regulatory requirements.

Failing to properly control access to an application means people who may not need access will have it, or too many privileges. It may mean that users or other applications can access information they don't need because of connections between applications or information sets.

Yes, we understand that IT often doesn't operate at the speed of the business. But it is up to senior management and the Board of Directors to determine which is more a risk to the company, slower to market or non-compliance and putting customer and other protected information at risk, effectively putting the future of the company at risk?

Are you ready to get serious about protecting your assets and your business?

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.