YOU RUSHED TO THE CLOUD—NOW IT'S TIME TO ASSESS AND ADDRESS CLOUD SECURITY

Don't Become the Headline.
Keep Your Customers and Your Reputation Safe.

UNISYS | Securing Your Tomorrow®

The pandemic prompted a rush to the cloud. Fast action was critical given the rapidly expanded work-from-home requirements and the need for touchless procurement, sales and service.

These efforts better-positioned businesses for the present and the future. A 2020 IDG study indicates that 59% of tech buyers planned to be mostly or all in the cloud within 18 months. If you're not in the cloud, you will be left behind in the race toward agility and innovation.

Now the initial rush has passed, and the dust is settling down. It's time to assess and address the compliance, cybersecurity, data privacy and risk implications of your cloud deployment. Cloud security and compliance continue to be the biggest pain points for cloud customers.

If you think it's too late for that, think again. It's never too late to do things right.

Doing things right is more important than ever since working from home has caused a surge in security breaches; more than half of legal and compliance leaders said that since COVID-19, cybersecurity and data breaches are their most-increased third-party risks; and up to 80% of CIOs and CISOs experienced a breach originating from a third-party vendor in the past year.

Here are a few tips on how you can do things right starting today—before you run into real trouble.

Embrace Security and Compliance and the Shared Responsibility Model for the Cloud

Choosing the right compliance framework is critical. HIPPA exists to protect Personal Health Information (PHI). The Payment Card Industry (PCI) standard protects credit card processing data. These are just a couple of examples of compliance regulations.

Your organization might be compliant, but that doesn't mean it's secure—and vice versa. So, in addition to your compliance framework, it's important to establish a security framework. Pick the right security framework for *your* organization. The security framework will provide a set of measures (controls) for people, process and technology governance. Example control frameworks are FedRAMP, FISMA, ISO and NIST-CSF.

As part of your security framework, understand and adopt the shared responsibility model. This will define the boundaries of what your cloud service provider(s) will handle and what you need to manage. The importance of adopting the shared responsibility model cannot be understated because your cloud hosting provider is not on the hook for compliance or security—you are. Adopt DevSecOps practices to ensure secure and compliant deployments.

Cloud security and compliance continue to be the biggest pain points for cloud customers.

Prioritize remediation to focus on fixes that minimize risk exposure.

Ensure—Don't Assume—Vendor Accountability in Your Supply Chain

Your IT environment includes more than just your enterprise. It also includes the vendors in your supply chain. Establish a set of best practices for sharing and securing data and ensuring compliance that cuts across organizational boundaries for your larger supply chain environment. Perform vendor risk management assessments before engaging with vendors. As part of this exercise, check international, national and state databases to make vendor risk exposure determinations.

Once vendors have passed those checks, be sure you are sharing information with these partners in a disciplined manner. The concerns remain the same whether your compliance and cybersecurity focus is internal or external. But the methodology is going to be different.

Identify and Address Your Points of Exposure

Establishing the right frameworks and models is key. Now you need to understand what's happening in your IT environment so you can take action to address gaps and incidents.

Start by understanding where your organization is exposed. Consider using automation tools to assess cybersecurity risk exposure by revealing holes in your cybersecurity strategy and IT landscape and their financial impacts. You may have a cloud server that isn't in conformance with your policy for password length and complexity. Available tools and services can help you to identify such gaps so that you know where to do remediation. Prioritize remediation to focus on fixes that minimize risk exposure.

Ramp up Your Cloud Security Know-How Through Training and Expert Partners

More than three-fourths of cybersecurity leaders surveyed in 2020 report said they're facing a skills shortage. It's even more difficult to attain and retain people with expertise in cloud security, which is the most in-demand cybersecurity skill set.

You may not have had time to recruit cloud experts in your rush to the cloud. And even now you might not be able to find, keep or afford them. That puts you in a high-risk position.

Train your team to ramp up their cloud security knowledge and skills. Seek partners with expertise in cloud security—that way, you won't have to manage the complexity alone. Employ available, advanced technology to supplement the resources that you already have.

Leverage AI to Scale and Focus on What Matters

Organizations on average use 25 to 49 security tools from up to 10 different suppliers. That creates a lot of noise in terms of alerts.

Consider leveraging Artificial Intelligence (AI) to cut through the noise and find the nuggets of information that are most important to you. This will help you to focus your energies on protecting your most critical assets and addressing incidents that pose the greatest threat to your business. Leverage AI-based Operations (AIOps) and automation tools to help accelerate decision-making. A recent Webroot survey found that out of the 800 IT professionals with cybersecurity decision-making powers they surveyed, 96% of them "now use AI/ML tools in their cybersecurity programs."

In the rush to the cloud, many organizations have cut corners. Maybe you have, too. That's understandable under the circumstances. The question now is: How do we get back on track?

Implementing the right security and compliance frameworks, adopting and understanding the shared responsibility model for the cloud, ensuring vendor accountability, addressing your points of exposure, ramping up your cloud know-how and leveraging AI will get you back on track—and safeguard your customers, business and job.

96% of IT professionals with cybersecurity decision-making powers use AI/ML tools in their cybersecurity programs.

Don't become the headline. Keep your customers and your reputation safe.

Learn More: www.unisys.com/offerings/cloud-services/cloudsecurity-and-compliance.

For more information visit www.unisys.com

© 2021 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.