pwc | United States

Four critical steps to better cloud security

Organizations aren't the only ones migrating to the cloud. Cybercriminals are going there, too, drawn by ever-increasing troves of valuable data. The challenge: how to protect it all.

Cloud computing offers speed, agility, scalability, and convenience. By 2025, enterprises will be doing as much as 80 percent of their work in a cloud environment, **one report predicts**. That's a lot of data—much of it highly sensitive—to leave unguarded, but many organizations are doing just that.

Unclear about who's responsible for securing cloud-hosted files, data, and applications under shared responsibility models, entities turn a blind eye to risk. With the cloud host providing so many services, they assume that security is taken care of, as well.

Who's minding all the data in the cloud?

According to **McAfee**, some 21 percent of files in the cloud contain sensitive data, including financial records, source code, and trading algorithms. Who's minding all this data?

Clients and customers entrust companies with their most personal information. It's incumbent on companies to protect it.

> Ultimate accountability lies not with the cloud host—but with the organization collecting and keeping that data for its clients, customers and business.

And indeed, **U.S. law** and laws in other countries—the European Union's General Data Protection Regulation, for example—place the liability for compromise of this data squarely on the shoulders of the organization that "owns" it. If a breach happens, the entity storing the information is subject to lawsuits or penalties, not the cloud provider.

The New York Department of Financial Services recently issued **new cybersecurity requirements** for third-party service providers to financial services companies. Other regulatory entities are expected to follow this trend, heightening scrutiny and tightening the screws on heretofore-unregulated service providers.

But, as with the NYDFS, agencies will most likely place the onus on the organizations contracting with these providers to be diligent and vigilant regarding third-party security and privacy practices.

There should be no confusion about who is responsible for keeping sensitive information safe.

> Cloud providers may have that "first line of defense" in place—the basic security intended to thwart hackers and thieves—but it's also up to the organization entrusted with that data to support it with risk and operational governance, processes and procedures.

Balancing speed and security

So should companies be doing more to ensure that the cloud environment they're using is sufficiently secure? The answer would seem to be yes.

Seduced by the promise of doing business faster and at a greater scale, organizations may turn a blind eye to the risks they incur by moving to the cloud.

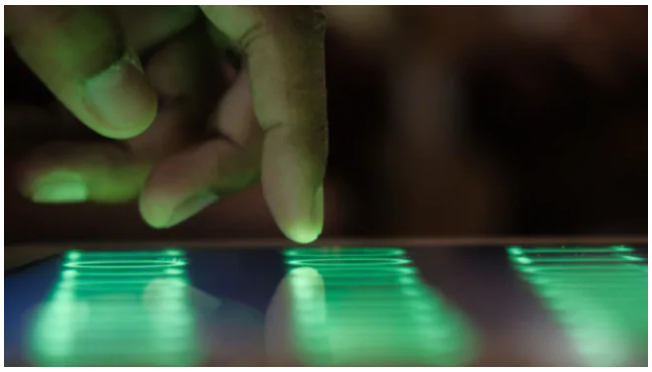
Sure, cloud providers do use sophisticated security measures to repel cyberattacks. And they update their technologies regularly, so enterprises don't have to. Cocooned against intrusions—or so they think—these entities forget that the cloud's enormous quantities of data and vast

attack surface make it at least as alluring to hackers as it is to businesses. The cloud's strengths—speed and convenience—could also be seen as weaknesses.

Too many organizations, lulled into a false sense of security, fail to check their cloud providers' safeguards or to supplement them with capabilities of their own. Complacency is bliss, it seems—until a breach happens, and organizational reputation, revenues and profits are subject to significant exposure.

This is the one-two punch we need to truly protect our most valued resources: the people and entities we serve.

Cover your assets: what you can do now



Race car and sports car manufacturers use high-performance brakes to let their vehicles travel as fast as possible—so that, when their drivers need to stop, they can do so quickly and safely.

In the same manner, organizations must design safeguards in their cloud environments at the governance level.

The difference between “risk” and “threats” can be subtle, but important. Here’s an analogy: Risk is what we encounter when we cross the street: If a car hits us, we could become injured. Threats are the possible manifestations of that risk, such as a driver speeding through the red light, coming directly at us, perhaps not seeing us because they are using their phone.

We can’t manage the threat, in this instance. We can’t force the driver to slow down, or to put down their phone and look at us. We can manage the risk, however, by making sure the street is clear of oncoming traffic before we cross.

Companies must manage risk—not just threats—so the business can take advantage of the speed and agility the cloud affords, while confident that security measures continually strive to mitigate the risks and exposures of a breach.

A four-step strategy for minimizing your cloud risk:

1. Incorporate cloud governance into your overall risk governance program

Too many organizations treat cloud governance as a separate entity, assuming that the cloud provider is protecting their sensitive information.

This mindset dates back to just a few years ago, when many used on-premises servers and internal, for-our-eyes-only cloud environments and IT merely supplemented business operations.

In today’s “connected age,” the on-prem model is quickly becoming obsolete. Stakeholder expectations and enterprises’ own business models demand instant access to services and data, which the cloud provides.

With the cloud having become an essential component of business operations, it’s imperative to fold cloud governance into overall organizational risk governance. Only then can the enterprise bring its full resources to bear on securing its cloud-hosted data and applications

from unauthorized access.

2. Plan for the worst

Being prepared for worst-case scenarios can enable an organization to respond quickly to threats and minimize damage to the business and the bottom line.

Organizations should already be doing this, and many are doing so in their risk governance/risk management practices. But moving to the cloud ups the ante: the old on-prem risk paradigms don't transfer to this new, complex ecosystem.

Businesses must envision a malware attack, DDOS attack, or data theft on the massive scale that the cloud affords, and design their processes and systems to withstand such an attack with minimal disruption to the business.

With hackers using increasingly sophisticated techniques to conduct and hide their nefarious activities, risk managers need to let their imaginations go wild and even a bit dark. "Expect the unexpected" is a great rule of thumb, and can help organizations to minimize their losses in the event of a cloud breach.

3. Know the impacts

Good risk governance includes understanding the full effects of a security compromise—critical for remaining calm in the proverbial storm that may follow, and for providing assurance to stakeholders.

A breach on the scale that the cloud affords can make for juicy news and sensational headlines, but oftentimes the impacts are minimal. So what if encrypted information was stolen, if it can't be viewed? Knowing the real-life effects of a security incident can help your organization avoid the damage that bad news reports can wreak on your reputation and revenues.

4. Focus on risks, not threats

As flashy as firewalls and red teams can be, cybersecurity—the "first line of defense"—is only as effective as its governance.

Just as critical, if not more so, is the "second line of defense," which is independent oversight of cybersecurity risks under a Chief Risk Officer or other independent risk executive. The second line should be positioned to pose a credible challenge to the CISO or IT Security executive operating in the first line, as well as to the cloud host. The second line should be providing independent oversight to aid in identification, mitigation, escalation, and remediation of risks where appropriate.

The buck stops with you

Speed doesn't kill, it's said; it's the sudden stop that gets you. And just as a fast car needs top-of-the-line brakes, your enterprise's fast-moving, ever-shifting cloud environment needs checks and controls that *you* design with your unique organizational challenges and priorities in mind.

"The buck stops here," former President Harry S. Truman said, refusing to shift blame for the country's problems. The notion holds true for the security of our data, as well, even when it's in the care of a trusted cloud provider. Placing your valued assets in someone else's hands doesn't give you permission to sleep at the wheel.

Let's talk

First Name (mandatory)

Last Name (mandatory)

Title (mandatory)

Company Name (mandatory)

Email address (mandatory)

What can we help you with? (mandatory)

By submitting your email address, you acknowledge that you have read the Privacy Statement and that you consent to our processing data in accordance with the Privacy Statement (including international transfers). If you change your mind at any time about wishing to receive the information from us, you can send us an email message using the Contact Us page.

Reset **Submit**

Shawn Connors
Principal, Cybersecurity and Privacy, PwC US
Email

Amandeep Lamba
Principal, Cybersecurity and Privacy, PwC US
Email

Michael Hodges
Managing Director, Cybersecurity and Privacy, PwC US
Email

Richard Kneeley
Managing Director, Cybersecurity and Privacy, PwC US
Email

© 2017 - Fri Sep 27 19:43:38 UTC 2019 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.