Published on *The National Law Review* https://natlawreview.com

Cloud(y) with a chance of incidents....

Article By:

Cynthia J. Larose

I hear this frequently: "We've moved everything to the cloud, so our security is good." Maybe yes, maybe no. Cloud applications operate on a "shared responsibility" model, which means that the cloud provider will have a certain level of security, but the customer also bears a level of responsibility for settings, encryption at rest, and a host of other issues. Misconfigured cloud storage applications (such as AWS S3 buckets) can expose terabytes of data to the open Internet. Bad guys know where and how to look.

Does your incident response plan deal with how to handle cloud incidents? (Do you have an incident response plan?)

Kroll has put together a helpful review of issues associated with cloud service providers.

> For organizations that have moved to the cloud, the so-called cloud management plane serves this purpose. Also known as the management console, administrator console or control plane, the cloud management plane is the web-accessible center for accessing and managing all the services and applications in the customer’s cloud instance. If access is not strictly limited or protected, an actor has the proverbial “keys to the kingdom.”

https://www.kroll.com/en/insights/publications/cyber/effective-cloud-incident-response?elqid=CDUFF000000899867

National Law Review, Volume XIII, Number 138

Source URL:https://natlawreview.com/article/cloudy-chance-incidents