NEXSEN | PRUET

Data Governance: Too Risky to Treat Like a Buzzword

Related Professionals

Angela O'Neal*
803.253.8210
aoneal@nexsenpruet.com

06.25.2020

Originally published in Columbia Regional Business Report June 22, 2020

Long before the COVID-19 pandemic, data security protocols like two-step verification and firewalls had become common and generally understood. Business leaders understand that in a cloud-based business environment, there's a real risk of nefarious actors seriously impacting your business. With more and more employees working from over the past few months, the threat from within is more defined than ever.

Consider risks such as employees storing documents locally on home computers or on personal devices. Do your people discuss business and proprietary information on non-enterprise tools? Do you? Using Zoom, What's App, Signal, Facebook Messenger, etc. create elevated levels of risk in and of themselves.

Think about it. With your business being conducted from living rooms, breakfast nooks and home offices, are your records and data being preserved? If not, can it be found or is it lost forever?

Data Governance

In academic terms, data governance is managing, accessing, using and securing information generated and used in your business enterprise. Governing corporate information is critical because it keeps data trustworthy and, in certain circumstances, helps it meet regulatory and legal requirements.

Most people in business are familiar with the axom "garbage in, garbage out." While true, consider the real stink that may arise if a well-intentioned employee mistakes a critical, valuable piece of information for garbage and discards it.

Common Example

We work closely with many lawyers and law firms, so a common example of how this can be a real problem is the "smoking gun." Something like an unknown email being produced at a critical point in litigating a business dispute. A solid defense can be turned on its head in seconds. Are you confident that all your employees are currently saving and archiving their emails, calls and text appropriately? Costly issues can arise even when your employees are honest.

During the COVID-19 pandemic, the demand for forensic collections is up and physical collection is down. Legal actions may be delayed, but they have not stopped. That pent-up demand will be creating pressures that are likely not being considered as businesses work to get back on site and back to full capacity.

Now, consider the hardship that could arise if that one staffer decides he has had enough and "goes rogue." Could he corrupt or destroy important data? Could he steal trade secrets or client lists? Could he mislead or lie to customers? If he did, how long will it take you to find out?

Three Ways

In real-world business operations, there are three ways to handle data governance.

The first is internally. Do it yourself. This is likely the least expensive up front. Just put a process in place, train your team and trust that they will do it right -- every time. This is the least effective way and often becomes the most costly.

The second option is to outsource the responsibility. The process can require investments of time initially and capital. However, it is typically the most risk averse and cost effective.

The third option comes after the fact. There are many forensic companies out there that can analyze your computers, phones, servers and determine most of what has happened to your data and information over a period of time. But, as you might imagine, the need for such comes when there is an urgent situation at hand. With urgency comes rising costs. For even the best forensic data team, recreating is inferior to capturing from the start.

Insurance of Sorts

Most businesses carry multiple insurance policies because insurance is the ultimate in risk reduction and mitigation. Forward thinking business leaders should consider data governance along those same lines.

At the very least, data governance will help prevent leaks and theft of sensitive information. More importantly, it can be invaluable in internal HR investigations. Imagine knowing the truth in those "he said, she said" situations.

If faced with an inquiry from a regulatory or enforcement agency, imagine the security that would come with knowing that all your records and data are correct and there's no chance that your company is going to be "caught in a lie" related to disclosure.

Finally, imagine a lawsuit where you are confident that there are no ticking time bombs waiting to derail your defense strategy.

Large businesses, particularly those in highly regulated industries, like banks and health care systems, have the largest needs for data governance systems. But the occurrences of 2020, has shone a light on the fact that there is very real risk that all business leaders should consider. Unless of course, your business only uses handwritten invoices, communicates via snail mail and only accepts cash payments.

Angela O'Neal is Director of Nextra Solutions, the information management and advisory service of the Nexsen Pruet law firm. O'Neal helps to reduce the risk associated with managing the large volumes of data created in today's cloud-based IT environments. Her experience as a civil litigator and as an investigator with the NCAA gives her invaluable perspective on the identification, preservation, collection, review and production of all manner of documents and information.