COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2021
Implement information governance to successfully manage ungoverned data

By Dean Gonsowski, JD

Dean Gonsowski (dean.gonsowski@activenav.com) is the Chief Revenue Officer of ActiveNav in Reston, Virginia, USA.

- twitter.com/dean_gonsowski
- linkedin.com/in/dean-gonsowski

Are we currently experiencing a data *explosion,* as many pundits claim? If the general volume of data is truly exploding, it is the longest and slowest explosion that we have ever seen. Despite the poor analogy, one thing is very clear: Organizations are struggling to control this growth of data, leaving them subject to significant compliance, privacy, and security risks.

As much as 90% of a company's data environment can be made up of unstructured data.[1] Unstructured data doesn't fit into predefined data models and is therefore inherently full of risk because it's hard to search, analyze, and control. No one knows what's hiding in this mess of data, which is often created by users and usually includes sensitive information that hackers look for, such as personally identifiable information (PII), Social Security numbers, and credit card information. Unstructured data is typically ungoverned, meaning that companies are sitting on huge amounts of risk, often unaware. It is a target for hackers because many companies do not know how much of it they have, where it's stored, or who owns it.

Meanwhile, the looming threat of data breaches continues to grow. Alarmingly, in 2020, despite huge investments in cybersecurity technologies, the number of reported data breaches was the highest on record. On average, the cost per record breached was $146. That cost went up to $150 if the record contained PII, which is still the most compromised type of record with PII being breached in 80% of cases.[2] Other significant costs stemming from security incidents (that should not be overlooked) include reputational damage and loss of productivity.

Companies, as they should, have been investing heavily in cybersecurity technologies like endpoint protection, identity access management, and third-party risk management to improve their security posture. Despite these prophylactic measures, data breaches continue to occur at an alarming rate, even at some of the most sophisticated companies in the world. For example, in January 2020, a Microsoft customer support database containing 280 million records was left unprotected, exposing email addresses and support case details.[3] If Microsoft, with all its resources, gets breached, it's clear that it's now a matter of *when* you will get breached, not *if*, which is a sobering thought, to say the least.