COSMOS
Navigate the Compliance Universe

Compliance Today - December 2021
How to successfully manage ungoverned data for risk mitigation

By Dean Gonsowski, Esq.

Dean Gonsowski (dean.gonsowski@activenav.com) is the Chief Revenue Officer at ActiveNav, located in the Washington, DC, metro area.

- linkedin.com/in/dean-gonsowski-2a469/
- @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 continuous explosion that we have ever seen. While organizations are struggling to control this data proliferation, they're also facing increased regulatory compliance issues, ranging from state-based privacy initiatives like the California Privacy Rights Act to New York's cybersecurity regulation, to even more novel regimes like Illinois's new biometric rules. In concert, headlong data and regulatory growth means an even larger burden for regulated entities in the healthcare, financial services, and energy sectors.

"Unstructured" data can comprise as much as 90% of a company's data environment.[1] Unstructured data is data that 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 dark data, which is often created by users and usually includes sensitive information that hackers look for, such as personal identifiable information (PII), Social Security numbers, and credit card information.

Simultaneously, the looming threat of data breaches continues to grow. Alarmingly, in 2020, despite huge investments in cybersecurity technologies, the number of compromised records was the highest on record.[2] 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.[3] Healthcare has been hit especially hard with compliance concerns during the pandemic. Today, healthcare data records are almost 50 times more valuable[4] than the next highest-value record, and the average cost of a data breach for healthcare institutions stands at $7.13 million—the most expensive of any sector.[5]

Cybersecurity alone is insufficient

Companies have been and continue to invest heavily in cybersecurity technologies like endpoint protection, identity and access management, and third-party risk management to improve their security posture—as they should. Despite these prophylactic measures, data breaches continue to occur at an alarming rate, even at some of the most sophisticated companies in the world. Certain sectors are being targeted at an even higher rate than average entities. For example, more than one in three healthcare organizations globally reported being hit by ransomware in 2020, with this sector experiencing a 45% uptick just since November 2020, according to *Health IT Security*.[6]

Information governance can complement cybersecurity efforts to help better manage information prior to and when the inevitable occurs. Information governance is the suite of activities and technologies that organizations

can employ to maximize the value of their information, while minimizing associated risks and costs. When done effectively, information governance reduces the amount of data under management and provides visibility into what data was breached if it occurs—or, rather, *when* it occurs.