Data Protection Policy Management Gets a Dose of AI

William Jan
VP & Lead Analyst

August 7, 2019

Among the highly regulated verticals, the defense industry possesses one of the most stringent supplier screening and qualification processes. With the US Department of Defense (DoD) elevating its cybersecurity requirements for contractors, and their subcontractors, to meet the 110 security controls of the NIST Special Publication (SP) 800-171 standard, vendors looking to sell to the DoD are leveraging AI to assist with increasingly complex compliance initiatives.

Important Details:

Becoming a government-approved vendor can yield great rewards to data and information providers. Once a contract is awarded and the provider obtains preferred government vendor status, the supplier could be looking at lucrative multi-year contracts that essentially make it immune to competition, very unlike the normal situation in an open commercial environment.

However, obtaining this status is undoubtedly harder than being a supplier to a typical corporate customer: Communication and data management standards, financial disclosure requirements, and third-party affiliation are just a few aspects of the required government screening. The latest compliance challenge faced by suppliers looking to partner with the DoD is due to NIST SP 800-171, a requirement that protects the confidentiality of Controlled Unclassified Information (CUI) in non-federal systems and organizations — effectively a cybersecurity measure. Failure to comply may disqualify vendors from supplying to the DoD and could result in removal from existing contracts for current government-approved vendors.

Since NIST 800-171 went into effect on December 31, 2017, there has been a struggle among government suppliers to comply simply due to the arduous task of aligning internal cybersecurity policies to those mandated by the DoD. The baseline version of NIST 800-171 includes 110 security controls for how federal government contractors — and their entire supply chains — must protect CUI. As mandated by those controls, organizations must implement and execute 30 information-security-based policies. Revision 2 of NIST 800-171, currently drafted and under review, only increases the scope, number, and complexity of policy-focused requirements. Many of these organizations throughout the DoD supply chain — especially small to medium-sized companies — may not possess the domain expertise, resources, or bandwidth to stay updated on the mandate's requirements and account for them.

Exostar, a cloud solution provider that helps companies in highly regulated industries mitigate risk with their business partners, has launched Exostar PolicyPro, a policy development and assessment engine. PolicyPro is powered by technology developed by ISMS Applications and leverages AI to track, align, and manage policies for suppliers who otherwise might have to turn for assistance to costly third-party consultants. The engine also assigns a compliance score to allow suppliers to monitor their risk exposure and potential shortcomings on existing policies while automating the development and evaluation of current and new security policies.

Analyst Rating: Positive

Strengths and Risks

The strength of Exostar comes from its business model and current global reach. The US government supply chain extends beyond domestic borders. The backbone of Exostar's platforms comes from deep aerospace and defense industry knowledge and experience along with a community network spanning more than 150,000 organizations in over 150 countries. Its business model is consistent: Strengthen security, reduce cost and risk, and increase productivity so its customers can effectively collaborate to better meet contractual, regulatory, and time-to-market targets.

The risk here is common to all those providing solutions into this space. While the US DoD maintains its list of government-approved suppliers, each is likely working with other subcontractors. For example, Raytheon, Boeing, Northrop Grumman, General Dynamics, and Lockheed Martin are just a few of the top US-based suppliers to the US DoD, yet these suppliers (defense contractors) maintain their own lists of subcontractors, many of which are non-US-based, such as EADS, Leonardo, Thales, BAE Systems, and Airbus Group. All these subcontractors, working on the same US DoD contract, would also be subjected to NIST 800-171 requirements. The advantage for Exostar is being able to leverage AI to support this proliferation requirement, enabling a mechanism for scalability, so primary contractors can effectively deploy the policy engine to their subcontractors.

Recommended Actions for Exostar

Exostar needs to continue to support its customers in deploying policy compliance assessments across the entire value chain. A method of doing so could include a platform that lets all members of a contract, foreign or domestic, review a common set of policy guidelines. More importantly, Exostar must obtain feedback from these global supply chain subcontractors — information that is critical for developing the next iteration of Exostar PolicyPro.

Outsell's Bottom Line

For the greater data, information, and analytics industry, Exostar PolicyPro marks another application in AI, this time in a highly regulated defense environment. One point of consistency in the use of AI in risk and compliance management remains niche applications, such as AppZen for expense policy management, and now Exostar for NIST 800-171 policy management. While other highly regulated verticals like financial services remain skeptical of AI applications on a broader scale (e.g., investment discovery), the fear may be fully warranted. Take pharma for example: Mistakes causing monetary losses in the billions from the wrong investment guidance or from a massive drug recall are almost more forgivable if made by humans than a machine. For now, it looks like niche applications of AI in risk and compliance management are picking up momentum, as proven by an audience that sets the bar the highest for trust: the government.

About Insights

About Outsell

Outsell is the only research and advisory firm serving information industry CEOs and their teams, and investors in media, tech, data and information. Our solutions are built from the ground up leveraging a unique set of assets: proprietary data, industry leading analysts, world class events, and a thriving and growing peer-to-peer community. Through deep industry relationships, we ensure our clients make great decisions for their businesses on a wide spectrum of topics, including competition and markets, operating and sales performance, M&A and due diligence, and critical trends. We stand by our work 100% and guarantee results. That's how fanatical we are about our clients' success.

Outsell inc.
Email: contact_us@outsellinc.com
Telephone: +1 650-342-6060