Stakeholders For Identity Security

A common refrain from CISOs faced with the identity security challenges of addressing non-human identities and agents is the inability to make significant changes in identity governance controls due to resistance from auditors and regulators. Second line assessors, internal auditors, external auditors and regulators have historically played a role in shaping the legacy identity governance controls for most enterprises. For a CISO to have concerns about the potential impact on auditors and second level assessors is understandable given the history of humans managing access for other humans. IAM systems have evolved to provide record keeping functions for identity management decisions satisfying the requirements of auditors year in and year out.

Today's challenges have more to do with the deployment of agents linked to existing identities (or not) rather than humans. I have three recommendations for CISOs facing the challenge of upgrading identity security controls for AI adoption:

1. **The decision to allocate resources to manage residual risk is yours and yours alone.** Every regulation, policy, law, regulatory guidance and framework reinforces the need for the security practitioner (you) to assess risk. That means that every second level analyst, internal auditor, external auditor and regulator carries the responsibility of determining if you (and your team) are doing "your job." They may contend that they understand risk broadly across enterprises (which has value to the enterprise as inherent risk) but only you and your team can truly understand risk and translate that into the allocation of resources to manage the risk.

2. **Second level, auditors, regulators are your identity security program stakeholders.** This means you must treat them as stakeholders but it **does not** mean you can't make changes in control design without their approval. You and your identity security team must adopt and implement new control capability to detect and identify agents, register them, and provide policy management for them in operation (guardrails). Given the need for designing new controls, you need to factor into your program the time to share feedback on proposed controls with your stakeholders and demonstrate receptiveness to understand their concerns. Internal and external auditors spend a large percentage of their time on identity governance control effectiveness in their annual reviews each year. They will need to add hours

in their planning process to consider the new controls and more importantly to understand them.

3. **When there is a significant change in technology (AI adoption) control design is essential.** This means that existing controls alone are insufficient to manage risk effectively given the fundamental changes in technology and how it is used. Pretending that existing controls (designed to manage human access to systems by humans) are suitable for managing agents is irresponsible for the security practitioner. New control design is essential to manager risk effectively. Reliance on humans in the loop for every access decision is neither scalable nor practical for NHI and agents. Teach your identity security team how to design identity controls using the new capabilities available in the market and reduce the dependency on humans to make decisions on provisioning, certifications and deprovisioning.