Chad Ballay

**Week 2**

**Problem Set**

Existing perceptions and process controls within in Global Limited are in scope for remediation and alleviation. These pain points are not limited to just this enumerated list:

* Overly burdensome process controls have yielded stakeholders bypassing security procedures.
* Branding and acceptance of the Security best practices is lower than needed for encouraging enterprise wide buy in.
* Unplanned incident responses are consuming department resources and consequently impacting business initiatives.

**Response**

*Tracking Data Across the Enterprise*

The company wide Enterprise Data Management initiative will have only a minor payback on ROI due to the need for continuous refinement. The inherent entropy will have to be combated through burdensome governance and compliance mechanisms. A coupling of this initiative to the broader Data Warehousing portfolio will help direct management focus. A dotted line alignment to a VP level position in the security area organization chart will give the access control supervision as required. Further refinement of this initiative should be explored by reviewing best practices as published by the EDMCouncil and other industry groups. (Enterprise Data Management, n.d.)

*Prioritizing Investments*

Program initiatives, budgetary allocations, and the ensuing expression of these by project focus and timelines should be moved up as a primary focus to the board level. (Heskett, n.d.) A top down approach will help ensure horizontal synergies are identified and acted upon. A long-term partnership with external consulting firms that focus on risk management should be explored. The value they bring in experience is also in addition to their role as an outside neutral third party. Compensation and incentive rewards should become a topline review item for the HR area to help align enterprise wide actions. (Berlich, n.d.)

*Implementing Security Controls*

Adoption of the internal division, CIS, provided Continuity Manager provides a many fold advantage. Primarily it’s use for role based access control will help to ensure NIST & ISO based standards can be readily adopted by Global Limited. Options to productize this as a SaaS offering and thereby creating an additional revenue stream should be socialized with the relevant stakeholders. The auditing of Authentication Manager usage will help ensure role-based compliance. Onboarding and other HR functionalities will need training and process adaptation. The now mandatory technical control of two factor authentication will prompt frustration but should be approached as a non-negotiable. The idea of a weekly or monthly newsletter highlighting data breaches could be done to help ensure buy-in.

*Reporting, Auditing, and Compliance*

As with Community Manager, the adoption of the internal platform CompScan as the enterprise SIEM solution has multiple key benefits. Providing a single pain of glass for viewing the threat horizon allows for tactical responses to be thorough and measured. Training and staffing prioritization should be given to SOC area so as to ensure onboarding of functionality. Third horizon initiatives within the Data Science areas can also initiated with regard to AIOps and other machine learning/automation efforts. (Ready or Not, AI Is Coming to IT Operations, n.d.)

Cross training with NOC and other telemetry based departments will allow for a greater degree of observability into the health and performance of core functionalities. Since this would be a new configuration of the horizontal teams a focus of internal promotions and cross training would be recommended for the short term. Blending these various platform tribes into a federation will yield more synergies than focusing on bringing in external candidates. Board level review and presentation should be given consideration for the next two fiscal years. The first fiscal year to ensure focus and the second fiscal year to ensure governance in place. Again, like the Continuity Manager, the CompScan platform should be socialized with relevant stakeholders to identify revenue potential.

**Synopsis**

The current response as laid out begins to address the problems of access control. Much of the above response is additional steps to capitalize on the inroads already being accomplished. This is not to be mistaken as criticism but as auxiliary controls to be implemented. Additional focus on bottom up buy in will help overcome systemic inertial barriers of adoption. Key champions can be identified and cultivated.

# Bibliography

(n.d.). Retrieved from Enterprise Data Management: https://edmcouncil.org/

Berlich, P. (n.d.). *How to Reward Performance for Security Professionals*. Retrieved from Information Security Magazine: https://www.infosecurity-magazine.com/opinions/how-to-reward-performance/

Heskett, J. (n.d.). *How Should Pay Be Linked to Performance?* Retrieved from Harvard Business School: https://hbswk.hbs.edu/item/how-should-pay-be-linked-to-performance

*Ready or Not, AI Is Coming to IT Operations*. (n.d.). Retrieved from Boston Consulting Group: https://www.bcg.com/publications/2019/artificial-intelligence-coming-information-technology-operations.aspx