Don't Give All of Your Data to Mikey!

Effective cybersecurity leadership requires more than demonstrating compliance with strong controls; it requires a level of *control design* as emerging technology evolves. Designing new controls to satisfy existing regulatory and industry standard requirements must be a core competency for CISOs/CSOs and cybersecurity leaders. Leaders must consider alternative ways of designing controls that do not depend on humans to process information, apply context, and then take appropriate remediation action. Feeding better information to humans to process and act on takes days, if not weeks, for remediation. This current model of feeding information to a person is growing in obsolescence primarily due to the high cost of staffing operations functions, such as a SOC or IAM operations team.

It is common practice for CSO/CISOs to consider a new cybersecurity product/platform and learn ways to improve their risk posture as a desired outcome. Inevitably, the CISO will instruct the prospective vendor to demonstrate the platform to one of the top SOC analysts, the SOC leader, or a senior security architect to compare with current capabilities. I call this practice the "give it to Mikey" step[1], named after a popular advertisement run by the makers of Life cereal in the 70's to encourage kids to eat cereal with less sugar. Mikey was the youngest of three brothers who ate anything and everything served to them, including cereal that was a healthy choice, much to the amazement of Mikey's older brothers.

Better cybersecurity control design that lowers operating costs and improves productivity is highly feasible today, but it requires an alternative approach to "giving it to Mikey." The objective is to reduce the unit cost of transactions through the use of data models (including Generative Artificial Intelligence) and automated workflows. Eliminating the need for people to take action for a subset of transactions by using pattern deviation to trigger an automated workflow lowers cost and increases the capacity of analysts to put more focus on high-risk events. This approach to control design increases employee satisfaction for SOC Analysts, Engineers, and IAM Administrators by enabling more analysis with less dependence on tedious tasks to complete transactions.

One way to accelerate this approach to control design is to utilize data science skills in the design process, both to improve data quality and to build models using machine learning (ML) systems that trigger automated workflows. Models don't take vacations, breaks, or weekends off. Models enable security event transactions in milliseconds, creating a first line of defense to the operation of an enterprise immune system responding to threats without the need for people to process information and respond with an action. The people involved become more vital to the enterprise by analyzing the transaction flows, making model adjustments, and focusing more time on higher-risk events/incidents.

CISOs have a growing number of options for using GenAI to improve cybersecurity practices today. More and more cybersecurity products are enabling control design using

[1] This advertising campaign was run by Quaker Oats breakfast cereal, Life, in the early 1970s

ML systems for enterprises, large and small. The majority of them continue the practice of "giving it to Mikey" and, to be fair, are instructed to do so. Resisting the temptation to follow this pattern is essential to achieve significant economic benefits from cybersecurity control design projects. CISOs need to give more explicit instructions for redesign efforts to substantially lower operating costs and improve productivity. This will force operations teams to consider ways to process transactions without people consuming data and making decisions. The more transactions that are automated, the lower the unit cost of the transactions. As a result, CSO/CISOs can then choose to improve productivity, increase capacity and/or lower operating costs.

Here is an example that is based on actual experience. A CSO asks the IAM Leader to consider ways to reduce the dependence on administrators to process access requests for several reasons, including:[2]

1. The volume of access requests is increasing by 25% annually
2. The existing approach requires increasing IAM operations headcount by 20% annually to keep pace with demand
3. Today, it takes many weeks for an access request to be fulfilled, and the time it takes to complete the transaction is increasing

The IAM Leader recognizes that conventional approaches to solving this dilemma will not yield substantial cost savings, and the CSO wants to lower operating costs for IAM Operations. The IAM Leader contacts several IAM governance platform vendors and learns of several ways to improve the systems/application integration challenges (like on-boarding applications). Unfortunately, there are no clear-cut methods for reducing operating costs while increasing capacity for access request processing. The IAM leader continues to search and speak to a management consulting firm that is willing to create an approach to this problem using data science.

The consultant identifies the need to assign a risk score to every enterprise network user based on the mix of granted entitlements that the users have and use. The consultant then assigns a score of 1-5 (1.00-5.00) for every user based on the analytic results of the entitlement usage work. The IAM Leader redesigns the onboarding process and entitlement request process by automatically approving all access requests originating from employees with risk scores of 3.50 or lower. Users with a risk score of 3.51 or higher who make an access request have to wait several business days for an analyst to approve the access request. The results from this project include:

1. 60% of the access requests are approved in milliseconds
2. The remaining 40% of requests are fulfilled within 3 business days
3. The unit cost of each transaction decreases by 50%
4. The capacity to handle new access requests increases by 25%
5. The level of satisfaction for the IAM Operations team members improves

[2] I used this approach, as a CISO, at three different enterprises and achieved the desired business benefits of lower cost and increased capacity

This scenario is only possible if CSO/CISOs avoid the tendency to “give it to Mikey.” Instead, CISOs need to focus on ways to rely on data science and models to trigger automated workflows while tracking the risk score for every user based on their online behavior. The best approach to getting these kinds of results is for the CSO/CISO to ask your team for substantial improvements in control design while lowering operating costs and increasing capacity. Have them pass this requirement along to the prospective vendors and seek their assistance in the control design. The most significant business benefits of cybersecurity control design come from reducing the dependency of transactions on people. “Mikey” will remain satisfied with whatever you give him, so don’t give him everything!.

https://www.youtube.com/watch?v=CLQ0LZSnJFE