Vendor Security Risk Management and Benchmarking

Executive Summary

Mitigating vendor security risk has always been a major challenge for organizations. Typically, there's no insight into the true nature of a vendor's best practices and overall cybersecurity posture on a continuous basis. While contractual compliance obligations may be well defined upfront, a piece of paper does not make an organization secure. To identify high risk vendors, the State of Missouri partnered with one of the leading security risk ratings companies to quantifiably track and monitor vendor security risk near real time. By instituting the vendor security risk management program, the State of Missouri has been able to demonstrably lower vendor risk. Using the same platform, Missouri can perform quantitative benchmarking against other peers to assist in answering the question, "how do we compare against others?".

While the State of Missouri has elevated its security posture over the last 5 years, one type of risk has remained elusive in monitoring and mitigating: vendor risk. While contracts establish security requirements and expectations with vendors, they do not shed visibility into the company's real practices and overall cyber hygiene. Vendors have been the initial attack vector in numerous breaches. Home Depot (56m credit card numbers), Target (40m credit card numbers), and closer to home a healthcare organization in Farmington, MO (48,000 SSNs incl. healthcare info) are just a few entities impacted by security lapses within their vendor partnerships. The State of Missouri's new vendor risk management program aims at mitigating known vendor risk by identifying compromised systems, unwanted user behavior, and cyber hygiene negligence.

The State of Missouri recently partnered with one of the leading external security ratings companies to gain access to their security ratings platform. The platform generates objective, quantitative measurements on an organization's security performance to produce daily security ratings from 250 to 900 (Figure 1). The platform analyzes existing security incidents and practices and applies sophisticated algorithms to produce these ratings which are based on externally observable, non-intrusive data and methods. The platform's ratings are based on terabytes of data from sensors deployed across the globe and include indicators of compromise, infected machines, improper configuration, poor security hygiene, and potentially harmful user behaviors. Organizations use security ratings platforms for continuous, objective self-monitoring, the monitoring of critical 3rd parties (competitors + vendors) and creating a simplified narrative with governing bodies about cyber security performance.

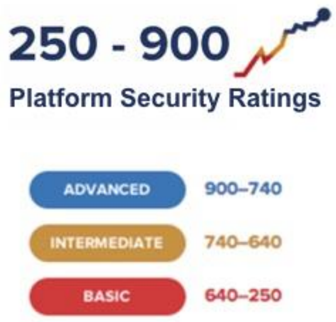

Figure 1

The State of Missouri is using this platform to reduce the overall vendor security risk. The state is also using detailed information from the platform to improve Missouri's overall security posture through benchmarking.

Vendor Security Risk Management and Benchmarking

Project Narrative

Concept

The chosen security risk scoring platform monitors thousands of organizations by using externally collected information. Their algorithm (Figure 2) collects data daily on compromised systems, diligence information, user behavior, and publicly reported data breaches and then outputs a grade (A-F) for the aforementioned categories and an overall organization score that closely resembles a credit score (250-900). The platform monitors thousands of organizations and monitored organizations don't have to be subscribers of the platform. Most of Missouri's vendor partners were already defined while some of the smaller vendors had to be defined. To define a new organization with the platform, known domain names are typically all that is needed. The platform's analysts will then research the company and ensure all known assets are included within the scoring. Based on the platform's findings, organizations with scores 400 or lower are 5 times more likely to experience a breach than organizations with scores 700 or higher.

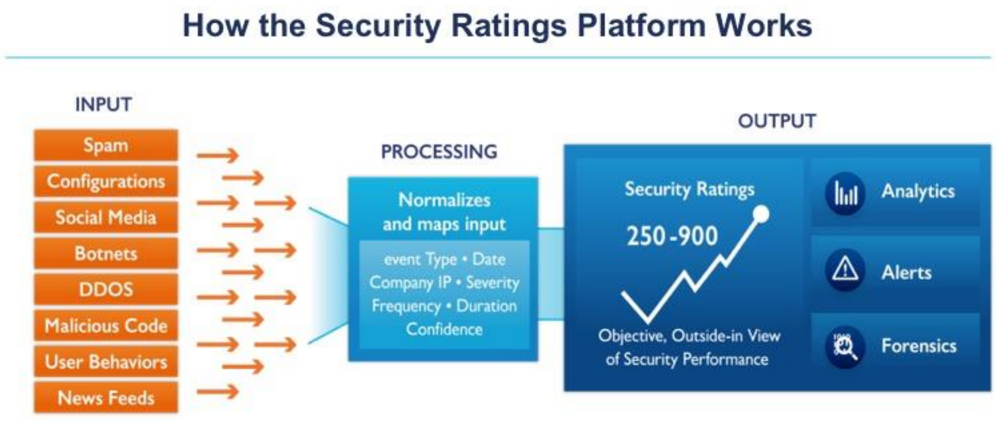

Figure 2

Significance

Organizational management increasingly needs to understand and mitigate its risks effectively to ensure long-term success. Effective risk management requires, among other things, a comprehensive and ongoing set of tools and processes to handle the dangers associated with third-party relationships. Cyber has been identified as one of the many risks a modern organization faces when partnering with a vendor. When an organization buys products or services from vendors, there's an implied level of overall risk reduction to business processes, but what's hidden under the surface may be an iceberg of cybersecurity risk that the organization wouldn't otherwise take on. While contracts can set general security expectations they cannot ensure that a vendor is continuously following security best practices. Performing security assessments against hundreds of vendors would be costly, time consuming, and in the end, unrealistic. The primary purpose of this project is to identify and assist in the mitigation of any risk to Missouri's data and services that is introduced by Missouri's vendor partners. The secondary purpose of this project is to quantify the State of Missouri's security risk and to ensure that it stays at an acceptable level.

Vendor Security Risk Management and Benchmarking

First party risk reduction

First party risk reduction was the initial phase of leveraging the platform. While knowing that vendor risk management was the end target, we needed to address our own measured risk first. The insights provided by the platform allowed us to quickly determine high risk areas that needed attention in our own house. Using the detailed data provided, we coordinated with various IT teams across the state to harden infrastructure and applications based on the platform's recommendations. One of the benefits of leveraging a platform that continuously monitors is that it can identify changes near real-time to an organization's security posture. While point-in-time assessments are valuable, having near real-time risk information about your organization is a key to any organization's success. The core of the effort took several months of work with most of the work falling into the hands of system administrators and application developers. As high risk areas were being addressed, our security score began to rise. Whenever there's a shift in our posture, the platform notifies staff.

Vendor risk reduction

As we were in the middle of reducing our own risk, we began focusing on our vendor community. The State of Missouri has hundreds of vendor partners, ranging from the Fortune 500s to small business owners in Missouri. After spending weeks combing through our vendor lists, talking with application development project leads, and prioritizing by criticality, we identified 50 organizations that we greatly rely on to deliver state services. If anything were to happen from a cybersecurity standpoint, it could have tremendous consequences to state government. With the 50 organizations added to our subscription, we quickly identified the outliers and then built a plan of action (Figure 3) to reduce their risk. All vendors tracked within the platform were notified by us directly about the program and its purpose. High risk vendors were given free access to the platform for 15 days to identify their problematic areas and to resolve them as quickly as possible. As their risk score changed, staff within OCS were promptly alerted to assist or to applaud the vendor's efforts.

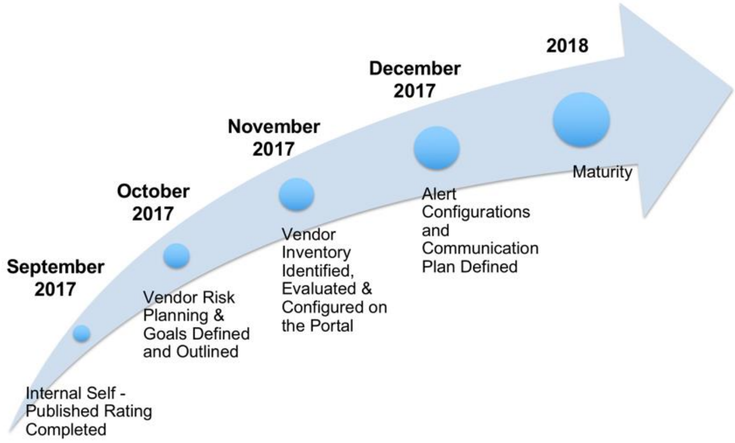
September 2017
Internal Self - Published Rating Completed
October 2017
Vendor Risk Planning & Goals Defined and Outlined
November 2017
Vendor Inventory Identified, Evaluated & Configured on the Portal
December 2017
Alert Configurations and Communication Plan Defined
2018
Maturity

Figure 3

Innovative

This project is innovative because it assists in answering two major questions: how secure is our vendor community and how does Missouri compare to other states and organizations regarding risk. Vendors generally don't allow their customers to assess internal and external resources on a routine basis but instead offer point-in-time reports and attestation information. While these are helpful, they don't get close to the true security risk that the vendor relationship may impose on the customer. Even if the customer could assess their vendors on a routine basis, it doesn't scale. This project delivers vendor risk insights near real-time to greatly assist with knowing where to shift resources to shore up any areas of concern.

Vendor Security Risk Management and Benchmarking

Over time, the questions “how are we doing from a security risk standpoint?” or “how do we compare to other organizations?” are asked often. While the government community tends to be one of the more transparent industries sharing stories and best practices with each other, it simply isn’t possible to perform quantitative benchmarking from within. Quantitative benchmarks enable organizations to measure their cyber risk, measure the impact of risk mitigation efforts, compare their performance against industry peers, and report security progress and results to key decision makers. This project supplies actionable quantitative metrics that drive key decisions around security investments and processes.

Impact

Reduced vendor risk

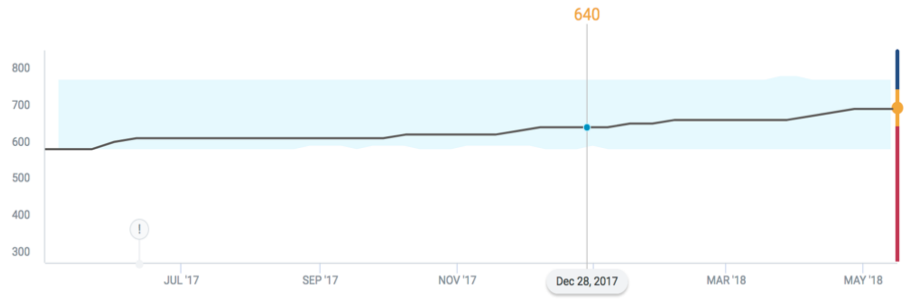

Figure 4

Since the inception of the vendor risk management program, we have demonstrably lowered our overall vendor risk. Since implementation through the end of 2017, we have seen multiple vendors make drastic improvements. One of our critical professional services vendors had a score of 580 and after we implemented our vendor risk management program, the score increased to 640 by the end of December 2017 (a 60 point jump, Figure 4). One of our key financial services partners had a score of 630 and elevated it to 720 after implementation (Figure 5). Overall, we have seen an average increase of 11.7 points across monitored vendors and within professional services, we saw an average increase of 30 points.

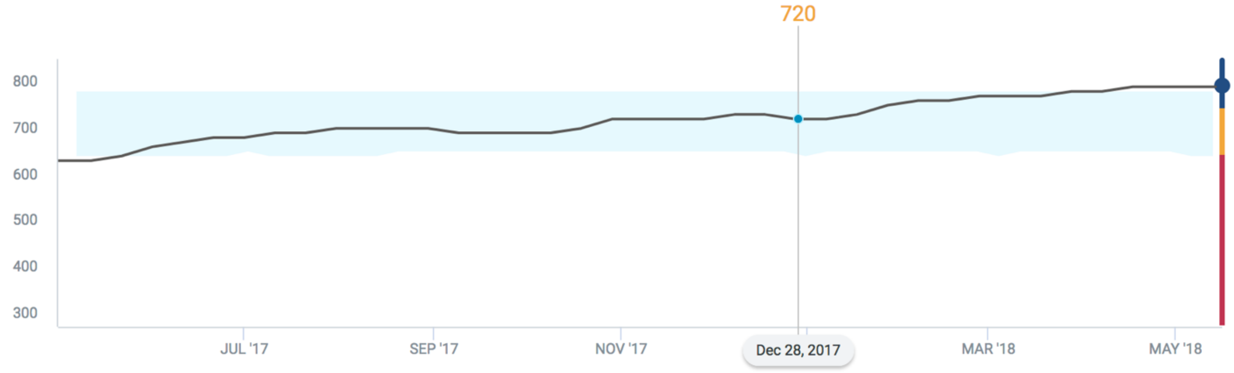

Figure 5

Reduced risk to state government

Due to the level of monitoring and visibility within the platform, the State of Missouri quickly resolved several high risk areas that reduced our overall risk drastically within several months. Our lowest score

Vendor Security Risk Management and Benchmarking

in 2017 prior to implementation was a basic level 610. By the end of December, our score rose 150 points to an advanced 760, the top tier of the platform's scoring. The State of Missouri is within the top 10th percentile in the government sector. The faint blue thick line represents the government industry range (Figure 6).

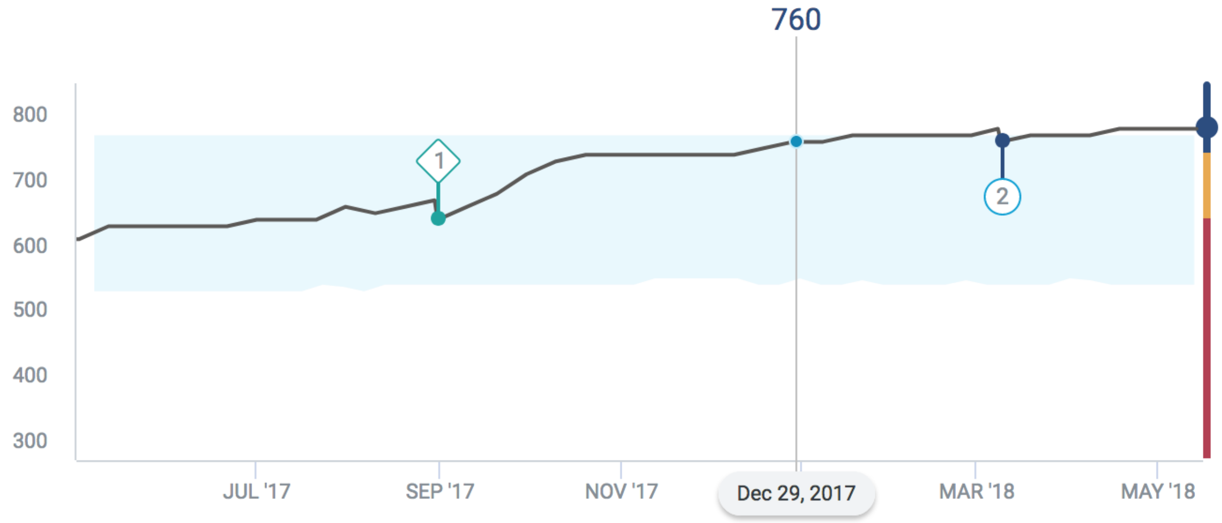

Figure 6

In September 2017, the State of Missouri started to break away from the government industry average (Figure 7).

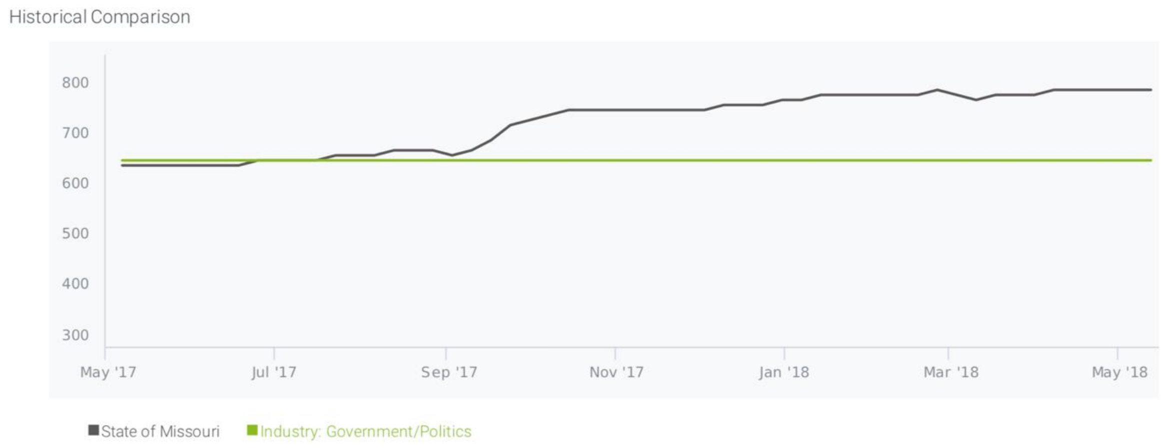

Figure 7

Vendor Security Risk Management and Benchmarking

The platform has changed the game in terms of benchmarking ourselves against other organizations. We can track Missouri's security risk against other organizations of similar size with ease to identify concerning trends that would in turn drive key investments and processes to keep Missouri in alignment or hopefully above our peers (Figure 8, Missouri is the top dark line).

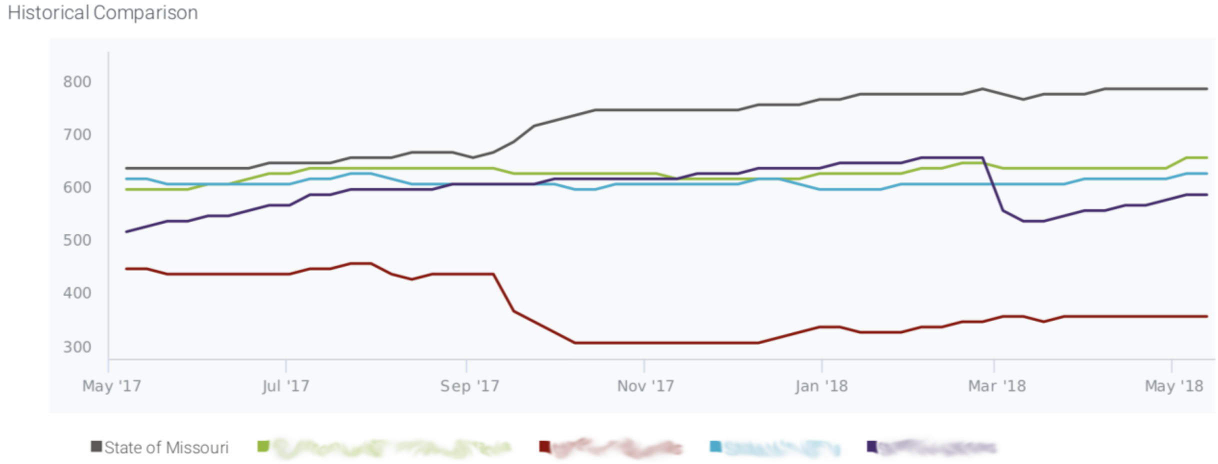

Figure 8