CASE STUDY: PHYSICAL SECURITY PROGRAM ASSESSMENT

Situation

Recently, a credit union came to RSM with a very big problem, and RSM responded with a very big solution. Credit unions are not only on the front line of cybersecurity as criminals increasingly take aim at smaller financial institutions, but they also face potential robberies and external fraud attempts. Over the last few years, these kinds of threats have grown significantly. To reduce its risk of crime and to protect its staff and premises, our client decided to take a deep dive into their physical security program.

Solution

To achieve a holistic yet detailed look at the organization’s security program, RSM created a custom solution centered on a physical security risk assessment and a physical threat assessment. The assessment focused on site-level as well as program-level risks to create a five-year road map for improving their security posture.

We began the assessment by interviewing the security team and learning how the current security program was structured. By the end of the interviews, we understood the people, processes and technology involved in the security program. The interviews also covered the current goals and challenges of the program.

Next, we interviewed key executives and lines of business, including the chief financial officer, chief operating officer, marketing team and corporate crisis management team, to understand the current goals and challenges for the business. This allowed us to tailor the new security program so that it would protect key assets and support the credit union’s business goals. This step is often overlooked, but it is essential to developing a security program that not only addresses risk but also supports the business.

Armed with program-level information and an understanding of the credit union’s business goals, we structured a set of assessments to gather exactly the information needed to form a plan to improve the security program.

The physical assessment began by looking at the security controls present at the buildings, covering processes and
technology. The RSM analyst considered public records, satellite imagery and social networks to gather as much information as possible before the guided walkthrough. During the guided walkthrough, our analyst and a representative from the organization entered the in-scope buildings and examined the entrances and exits, security staff and guards, cameras and alarms, and other security controls. Our analyst attempted to enter areas without the proper credentials in order to test the security controls and processes. After the walkthrough, the analyst identified the observable weak points and provided recommendations based on regulatory requirements, industry best practices and the limitations of the actual sites. All of the advice was grounded in the observations made at the locations and based on the analyst’s experience.

Next, we looked at the threats presented by the buildings’ environments and geographical areas. Human threats such as crime and terrorism; natural threats, such as storms and earthquakes; and technological threats, such as traffic and derailments, were all considered for each location. After gathering the threat data, the primary threats for each location were identified and locations were grouped into high, medium or low levels to understand the severity of the threat. Having established the threats, our analyst then determined the impact of these events combined with their likelihood to calculate the actual risk each location faced.

Results

Having identified the threats faced by the credit union and analyzed the security controls in place, we then assessed the risks the organization faced and developed a multiyear plan to align the security program so that it protected key business processes and supported the credit union’s long-term goals. The recommendations were presented in a phased approach with costs and importance clearly indicated. The credit union understood which improvements would have the greatest impact given the cost and effort involved in making them.

To make the long list of recommendations more manageable, we organized them around several key goals and developed a timeline for achieving those goals. For example, the goal of “building a key management program” could be accomplished by implementing three specific recommendations in a two-year period. To achieve the goal of “strengthening security operations” we provided eight solutions to be rolled out over the next four years.

Each recommendation was marked as high, medium or low priority and an estimated cost was listed wherever possible. We provided an illustrated timeline of the plan as well as detailed explanations of each recommendation to give the credit union a clear visual of the overall road map along with the specific, practical steps to achieve their goals.

Although the client was already aware of some of the gaps in their security program, RSM was able to identify areas for improvement that were not well understood before the assessment. For example, we made a number of recommendations for how to achieve the goal of “strengthening vendor management” that illustrated that the current vendor assessment polices were spread over too many departments, lacked cohesiveness and that the vendor processes should be centralized to strengthen security.

The client was also surprised to see the amount of risk they accepted due to the high crime rates in the areas around its buildings. We identified ways the credit union could increase the safety of their employees by changing policies, consolidating security responsibilities and improving the security infrastructure in the employee parking lots and garages.

Credit unions face many security challenges, few of which have simple solutions. To develop a mature security program, an organization needs more than a list of problems and fixes. Our service not only identifies security gaps, but also determines the actual risk and potential loss of each gap and prioritizes the solutions based on that analysis. For those solutions that require multiple improvements over time, we provide a phased plan for how to achieve each goal. With this plan, security managers can answer the “how” questions from their staff and the “how much” and “how long” questions from the executive suite. By comparing the risk and potential loss to the projected cost of the solution, a client can identify changes that have the quickest and greatest impact.