Implementing a Risk Assessment Program to Help Protect Your Branches

By Mary A. Gates, CFSSP, CHPA-III

Overview

Banks and other financial institutions are faced with the critical challenge of ensuring the protection of their people, assets and information. Security Officers should utilize an ongoing assessment program to monitor and respond to changing risks and threats. Known as a Risk Assessment Program, the methodology utilized can be both facilities-based and incident-driven, considering all known sources of influencing information for the identification of risks as well as the examination of severity, frequency and operational impact. Areas of examination should include but may not be limited to: crime statistics, site incident history, neighborhood factors, nearby competitor security features, regulatory requirements and property issues. All identified risks are examined and mitigated individually with documentation maintained in department databases and reassessments driven by changes in the environment.

It is important to note the Risk Assessment differs from a Security Review. A Security Review assess how effectively your bank's security policies and procedures are being implemented, uncovers where security gaps exist and helps identify issues driving non-compliance with the Security Program. The Risk Assessment will identify your most critical resources and the weaknesses that can be exploited along with the likelihood of occurrence.

Approaches to the Risk Assessment Process

Within the security industry there are quantitative and qualitative approaches to Risk Assessment and mitigation.

- The quantitative approach involves scoring risk factors via a point system that ranks facilities by their overall score in order of risk concern.
- The qualitative approach involves a similar analysis process but without the scoring and, instead, a focus on the identification of specific risks and the implementation of successful mitigation techniques without consideration for any arbitrary scoring or ranking against other sites.

Some banks have taken an approach that it is most important to focus on solutions and, accordingly, use a customized, qualitative process that analyzes facilities individually and incorporates the occurrence of incidents initially and one at a time.

Mitigate Risk through a Comprehensive Evaluation of Threats, Risk and Vulnerabilities

From insider threats to external forces, it is important for security professionals to remain vigilant in their understanding of the risks, threats and vulnerabilities in and to their organizations. The methodology begins with the identification of the business to be conducted at the facility and its associated risks, analyzing the seriousness and frequency of those risks and then identifying and implementing the best mitigation options. This is known as a **Facilities-Based Process**. Risk for facilities is assessed in two parts: a pre-construction review and an ongoing, steady-state program. In pre-construction, it is assumed that certain base-level security protections will be implemented for the given business type under review. As an example, all branches of your bank, regardless of risk profile, will receive alarms, vaults, and lobby video surveillance systems.

On an ongoing basis, the steady state process requires that a current assessment for each facility be maintained on file with updates completed according to a defined process and as dictated by the frequency of major incidents. For simplicity, updates are required during steady-state when indicators point to a possible change in the level of risk or a change in the assets and people exposed. This can include the occurrence of a major event, a change in business function, knowledge that nearby criminal activity has increased, or that property changes have taken place, including modifications to building design or equipment (such as the addition of an ATM).

Employing an **Incident-Based Process** methodology involves the consideration given to the need to reassess the risk to facilities and to analyze the risk to individual staff following any major incident. This is done to confirm whether major events (i.e. an armed bank robbery) will or will not, on their own, dictate changes in protection packages. These Risk Assessments can trigger short-term or temporary solutions to protection packages or point toward the need to reassess general safety and possibly redesign facility protections. Security staff are required to consider the need for reassessment during their post-incident review and to implement such assessments or reassessments as deemed necessary.

What are the Differences between Threats, Risks and Vulnerabilities?

You may be thinking, "I thought threats and risk are the same. What do you mean when you talk about vulnerabilities?" Threats, risks and vulnerability are not interchangeable terms. Rather, they are the essential ingredients of an accurate risk analysis. In their simplicity,

Threats:

- Need to be identified
- Generally, cannot be controlled

Risks:

- Can be mitigated
- Can be managed to lower vulnerability or impact on the business

Vulnerabilities:

- Can be treated
- Weaknesses should be identified
- Proactive measures should be implemented to correct identified vulnerabilities

What Steps Can I Follow to Assess the Risks to My Branches?

Once you decide to implement a Risk Assessment Program at your bank, you should outline the steps of the Risk Assessment process you will follow, detailing how the careful evaluation of the business purpose, threats, risks and potential solutions comes together to provide for the safety of individuals and the protection of assets and information. At a minimum:

1. Identify the **EXPOSURE** in order to identify the areas of risk. The starting point to consider when examining risk is the type of business being conducted at the site under review. By identifying the business type, the staff, assets, and information at risk are more clearly identified. And those exposures must be clearly in mind when considering the likelihood and severity of potential attacks. For example, a facility that handles cash takes on risks associated with that function, such as the risk of robbery, which other facility types may not experience. The risk to staff and the potential loss of assets are clearly seen when the assessment process begins with a look at the business type. This step is an efficiency in the review process that helps focus the reviewer on the most likely risks as opposed to a lengthy general review of all risks.
2. Identify the **THREATS** associated with the facility type. Once the business type has been identified, then the review can be focused on the most likely risks associated with that business type and the corresponding exposures. Examples of threats for branches could include robbery, bomb threats, violence in the workplace, information loss, etc.
3. Examine the **LIKELIHOOD** and **SEVERITY** of attack. Reference internal and external indicators: crime statistics, neighborhood conditions, incident history, incident trends, Security's knowledge, consideration for what protection strategies other financial institutions are using, etc. By researching all possible sources of information, the degree of risk – both its likelihood and severity – can be gauged by the reviewer. All these factors drive whether the exposures are under significant risk of attack.

4. Evaluate the **ADEQUACY** of the existing **PROTECTION** package. Once the risks to the exposed people/assets/information are identified, the reviewer must consider whether the degree of risk (likelihood and severity of attack) warrants adjustment to the current protection package. This requires that each risk be examined one at a time to evaluate whether existing protection will provide an adequate safeguard. If the protection level is adequate, then no further action is necessary, and the assessment can be concluded. If any gaps or weaknesses are identified, then solutions and an action plan must be developed.

5. Identify appropriate **SOLUTIONS** to gaps in the protection package. Enhancements, upgrades, etc. may be required to further harden the branch. *However, solutions must be appropriate to the risk and effective in mitigating the frequency and severity of the risk.* As an example, installing bullet-resistant glass at the teller line is not an appropriate solution to address a noted increase in risk associated with customer theft after-hours at the ATM. Instead, the installation of video surveillance cameras and security lighting enhancements or a re-lamping of broken fixtures is likely a more appropriate solution.

6. Once you have identified the solution and developed pricing, **CONFIRM** the mitigation plan with the impacted business unit(s). It is not uncommon to present a risk mitigation plan only to learn the site has been identified for a relocation project, remodel or is being closed. Therefore, it is important to take the time to inquire as to any business drivers that might require a modification of the solution or place the entire plan on hold, either temporarily or permanently. Safety is the priority, but a good Corporate Security business partner can always find an interim solution for sites in a state of transition.

7. With agreement on the decision to move forward and an implementation plan at hand, initiate and follow through on the **APPLICATION** of the solution. Work with vendors, project managers, etc. to drive the projects to completion.

8. It is important the installed solution is **TESTED** and **VALIDATED** as functional and beneficial for the intended result post-installation and in the real workplace environment.

In closing, the Risk Assessment is not a one-time review. The world continues to evolve as does your organization. Risk analysis is complex, and the threats are always there. Security measures, processes or procedures put in place three years ago may not address the threats and risks your organization faces today. Understanding the magnitude of the consequence associated with those threats and risks, their likelihood to occur and the possible effects on your bank are the primary components to managing security risk at your bank.

- Article by Mary A. Gates, CFSSP, CHPA-III

Mary Gates is a Vice-President of GMR 410, LLC a risk-solution security consulting firm and wholly owned subsidiary of GMR Protection Resources, Inc. Learn more about GMR 410, LLC by visiting their website at www.gmr410.com