Implementing a Physical Security Risk Assessment Program to Safeguard Employees, Customers and Assets

October 13, 2021

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410
Trusted Advisors | Trusted Solutions

Email: marygates@gmr1.com
Cell: (504) 228-4829
www.gmr410.com

Mary A. Gates, CFSSP, CHPA-III

Vice-President, Security, GMR 410, LLC

- More than 30 years in Corporate Security
- Retired as Executive Director for Global Security at top banking firm
- Extensive physical security, technology, investigations and project management experience
- Former Member ABA Bank Security Committee and Briefing Advisory Board
- Currently serving as Advisory Member ASIS Banking & Financial Services Committee

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Who is GMR 410?

- Wholly-owned subsidiary of GMR Protection Resources, Inc
- Full-service risk management security solution consulting firm
- Diverse Supplier, Certified Women-Owned Business
- Faith, Integrity and Quality are our core values
- Independent
- Proactive and client-oriented
- Credentialed and affiliated with major banking and global security organizations

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Disclaimer

The information, including opinions and views expressed herein, are those of the presenter. They do not necessarily reflect the views of GMR Protection Resources, Inc. or GMR 410, LLC.

The content is presented for educational and informational purposes. The presenter is not an attorney and is not rendering legal advice. The presenter, GMR Protection Resources, Inc. and GMR 410, LLC have no liability to any persons or entities with respect to any loss, liability or damage alleged to be caused by any reliance on information provided in this presentation.

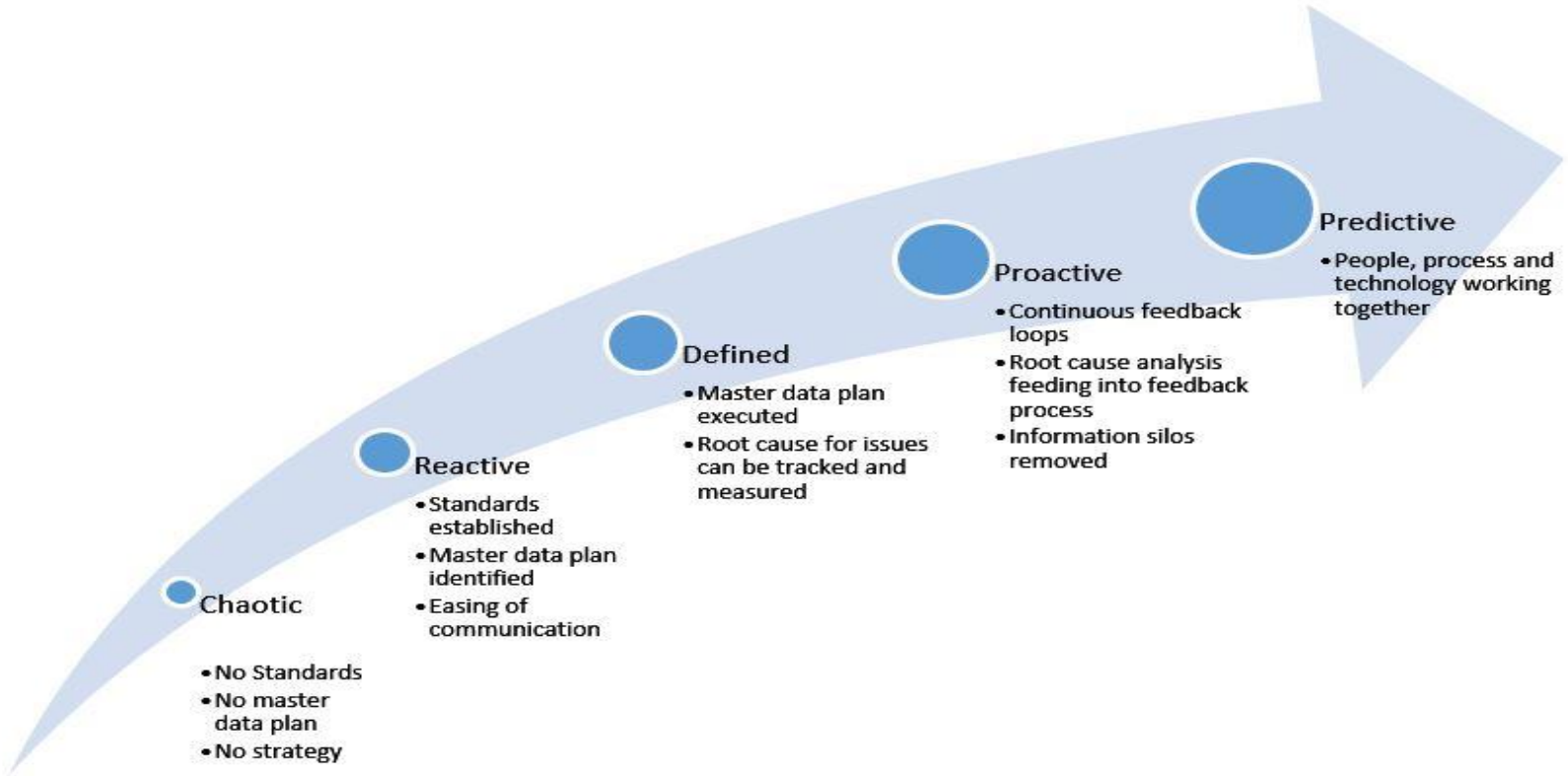
certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Objectives

Understand

- Why security personnel need to conduct initial and on-going physical security risk analysis
- The difference between risk, threats, and vulnerability
- Approaches to the risk assessment process
- Key steps to assess and manage risk



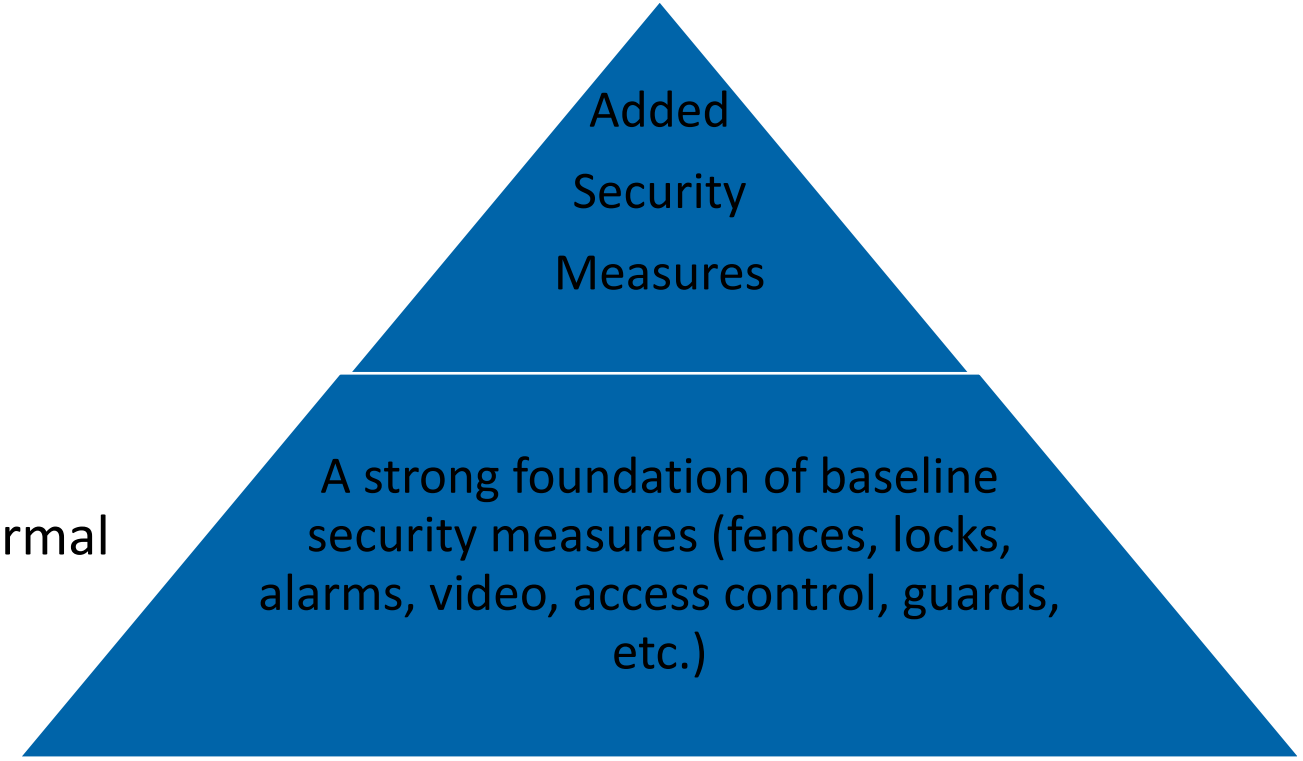
certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Introduction

The 4 most common approaches to the implementation of security

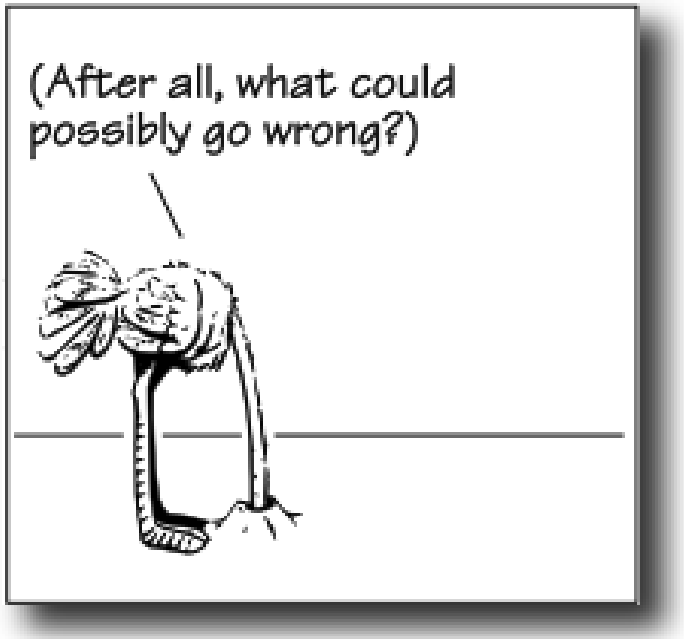
1. Baseline Security
2. Packaged Security
3. Security Vulnerability Analysis
4. Security Measures Based on a Formal Security Risk Analysis



certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Why Conduct Risk Assessments? The Benefits



- Become a strategic partner
- Proactive, not reactive
- Site selection
- Prioritize your security spend across your locations
- Guide operational decisions such as branch or building design, type of ATM, hours of operation and service times
- Establish security operational policies and protocols
- Highlight areas in which greater (or lesser) security is required
- Assemble some of the facts needed for the development and justification of cost-effective countermeasures
- Duty of Care

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Differences Between Risks, Threats and Vulnerabilities

- Risk
  - The potential for loss, taking into account likelihood, impact and vulnerabilities
- Threat
  - A source of potential harm
- Vulnerability
  - A weakness or flaw in a security system or any business process that could conceivably be exploited by a threat

- Risks
  - Can be mitigated or accepted
  - Can be managed to lower impact on the business
- Threats
  - Must be identified
  - The Adversary
- Vulnerabilities
  - Identify weaknesses
  - Can be treated

Examples of Risk Faced by Banks

- Financial loss
- Business interruption
- Physical risk to people
- Loss of consumer confidence
- Brand image / Reputational harm

- **P**olitical / People
- **E**conomic
- **R**egulatory
- **F**inancial
- **O**pportunities / Outcomes
- **R**eputation
- **M**anagement
- **A**ssets
- **N**ew Partnership/Project/Contract
- **C**ustomers
- **E**nvironment

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Important Messages

- Perception
  - Involves people's beliefs, attitudes, judgements and feelings as well as social and cultural values and the disposition that people will naturally adopt toward different hazards and threats
    - Utilizing a cross-business approach and verifiable, statistical data helps reduce / eliminate the bias and drives a consistent, methodical approach

- Foreseeability and Negligence
  - Not all risks can be identified but security managers, their management and the bank Board of Directors may be judged negatively after an event if there should occur a reasonably foreseeable undesirable event which should have been anticipated and mitigated

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Approaches to the Physical Security Risk Assessment Process

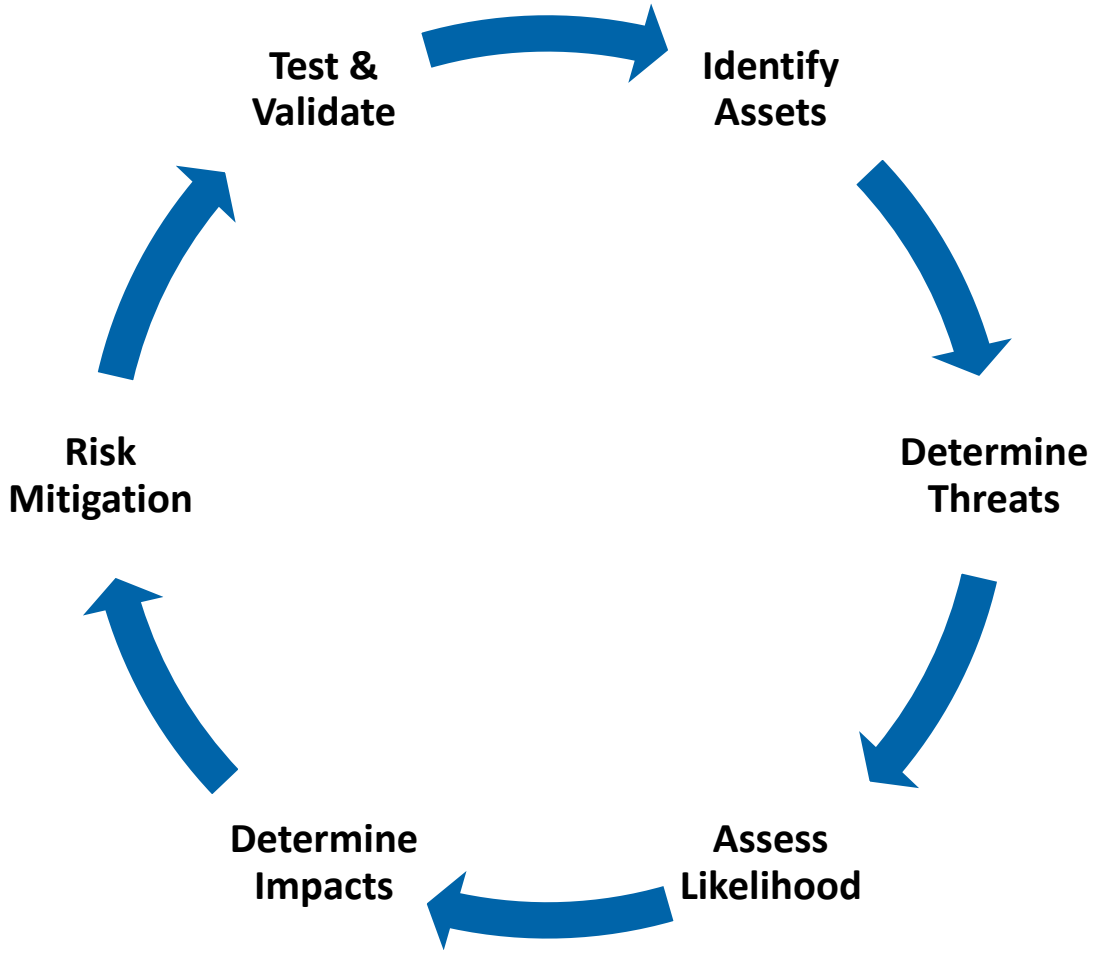
- Facilities-Based Process
  - Pre-construction
    - Certain base-level security for all locations
      - ✓Example: all branches, regardless of risk profile, receive alarms, vaults and lobby video surveillance systems
    - Assessment during Pre-construction may identify need for additional security
  - Ongoing, steady-state program
    - Current Assessments on file
    - Updated when change in risk, assets or people exposed

- Incident-Based Process
  - Reassess risk following any major incident
  - Completed to confirm if a change in the protection strategy is needed on a short or long-term basis
    - Example: an armed bank robbery by a serial bank robber may result in the temporary placement of GPS trackers in the market

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Risk Assessment Model



Identifying the Assets

Identify the assets that require protection in order to meet business objectives

Tangible

- People
- Property
- Documents

Intangible

- Information
- Some Intellectual Property
- Operational Continuity

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Determine the Threats

- Characterize the threats
  - Requires an understanding of the environment and context in which the business exists
  - Target attractiveness is a key threat consideration in countering crimes against banks

- The 3As
  - Adversary – who may seek to cause harm?
  - Asset – which specific asset(s) are at risk of becoming a target?
  - Action – what is it the adversary may seek to do?

Assess Likelihood

- How likely an adverse event is expected to occur
  - Historical factors and incident / crime records
  - Asset attractiveness and value to an adversary
  - Asset location
  - Proximity of, and accessibility to, sources of threat
  - Environment in which the asset exists
- Measured
  - Simple *low, medium, high* scale or
  - 5-point scale (see right)

	Likelihood
5	Happens on a regular basis or is considered likely to occur in the near future
4	Happens from time to time or has the potential to occur in the near to mid-term future
3	Has happened previously in this location or area or is assessed to have the potential to happen in the future
2	Is not known to have happened previously in this location or area but possibility of occurrence in the future cannot be discounted
1	Has never happened and is highly unlikely to happen in the future

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Determine Impact

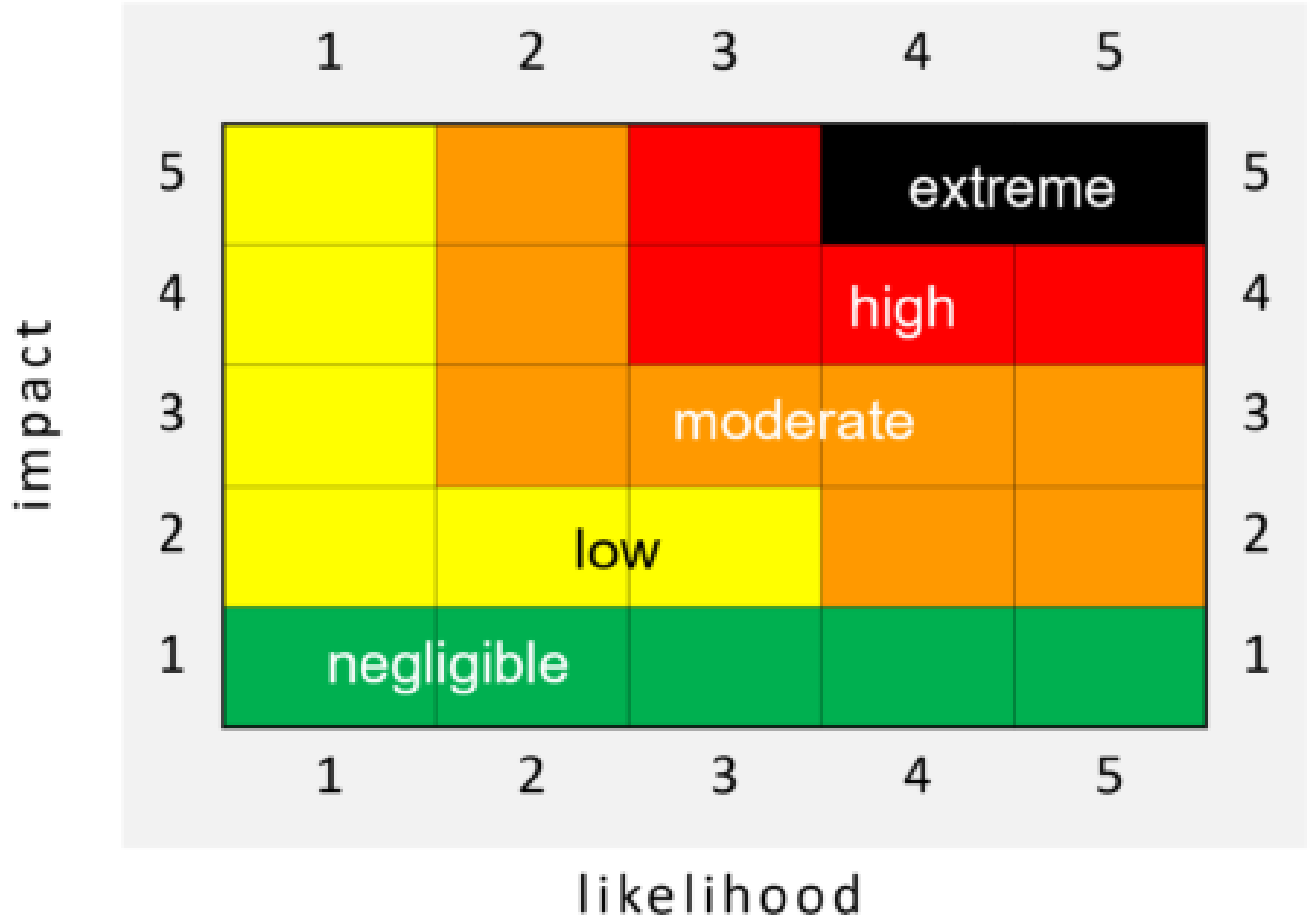
- Different from book value
  - Reflects the true value of the asset to the bank at any given time
- Direct loss
  - Immediately attributable to the adversary action
- Consequential loss
  - Loss that builds up as a result of an adverse event due to non-or reduced operability
- Measured
  - Simple *low, medium, high* scale or
  - 5-point scale (see right)

	Impact
5	Exceptionally grave consequences, such as extensive loss of life, widespread severe injuries or total loss of primary services, core processes or function or irreparable damage to reputation
4	Serious consequences, such as loss of life or serious injuries, impairment of core processes and functions for an extended period of time, or serious reputational damage
3	Moderate to serious consequences, such as injuries, impairment of core functions and processes, and some reputational damage
2	Moderate consequences, such as minor injuries, minor impairment of core functions and processes or slight reputational damage
1	Loss or damage of the asset would have negligible consequences or impact

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Risk Matrix – Likelihood vs. Impact



certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Risk Mitigation

- TEAR – Transfer, Eliminate, Accept, Reduce
- Evaluate adequacy of existing security protection package
- Identify appropriate solutions to gaps in protection package
- ALARP - “As Low As Reasonably Practicable”
  - Mitigation strategy must be both risk and cost-commensurate
- Consider corporate culture and be prepared to encounter resistance
  - Negotiating and interpersonal skills are paramount
- Key limitation concerns
  - Customer access and expectations
  - Fire/Life Safety codes
  - Budgetary constraints

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Implement, Test and Validate

- Move forward / implementation plan
- Solutions must be tested and validated as functional and beneficial for the intended result
- Document results on a location's *Security Risk Scorecard*
- Review each location's *Security Risk Scorecard* at least annually
  - Measure and report effectiveness of the program
  - Verifies controls have been implemented and are effectively mitigating risks as expected
  - Provides regular monitoring for changes to the environment that may alter a location's risk profile

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

Sample Physical Security Risk Scorecard

Risk	Source(s)	Possible Impact	Alleviating Factor(s)	Aggravating Factor(s)	Likelihood/Impact	Priority	Action Required	By Whom	When
Employee Fraud at the ABC Branch	Manipulation or access of customer data by lone or colluding employees	Direct losses averaging $5,000 over the last 2-years. Reduction in hours leading to skimming of teller drawers and further growth of fraud due to decline in economic conditions. Risk of fraud culture.	Stable employee and branch management relationships. Problematic employees guilty of fraud terminated. Network threat hunting program scheduled for roll-out 2Q2021.	Branch manager often offsite due to job requirements resulting in limited direct and consistent daily oversight. Delays in installing TCRs and network improvements leave access to cash and systems vulnerable.	Likelihood =3 Impact = 3	Moderate	1. Continued Monitoring 2. Re-assess when threat hunting program is installed	1. Retail Management 2. Security	1. On-going 2. 2Q2021
Bank Robbery at the ABC Branch Teller Line	Armed Serial Bank Robbery Suspects Operating in the Geographic Area	Direct losses averaging in excess of $50,000 due to accessing top and bottom drawers of all tellers, and forcing tellers to escort suspects to vault, during robberies over the last 12-months. Employee injuries, reduction in employee morale possible and further eroding in confidence from the employee base.	Additional lobby cameras and entrance cameras installed. Additional bank robbery training completed. GPS packs installed at the teller line and in the vault.	Branch hit following installation of additional security measures with 1 minor injury. Banks in immediate area operating with enhanced protection packages (armed guards, SEVs, BRG) are not being attacked. Branch located on main thoroughfare with police response in excess of 3 minutes.	Likelihood = 4 Impact = 5	Extreme	1. Place off-duty police officers on site pending installation of bullet resistant glass 2. Install bullet resistant glass 3. Remove off-duty police post installation.	Security	Place off-duty police officers on site immediately. Submit capital expenditure funding package for bullet resistant glass installation within 10 business days with project plan to complete installation by vendor no later than 90 days following approval of capital expenditure.
Hook & Chain Attack at ABC Branch Drive-Up's XYZ-Type Name of Manufacturer ATM	Damage to ATM and theft of cash by criminal gangs	Direct loss in excess of $200,000 average cash balance in ATM + consequential loss due to severity of damage to the ATM and loss of revenue due to time to repair or replace machine.	Tracker inside of cassette to help track cash. Internal and external video surveillance cameras to provide suspect images. ATM located on island pedestal with bollards on 4-corners.	Tracker and camera are not pro-active deterrents. Bollards have not proven effective in preventing attacks on this type of manufacturer's ATM. The suspects are able to weaken the hinges with a grinder, use a hook & chain and quickly defeat the maching utilizing a design defect.	Likelihood = 4 Impact = 5	Extreme	Coordinate with ATM group to install blocker or replace ATM.	ATM Group	12/31/2021

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

In Closing

- Not a one-time review
  - Re-assess risk
    - On a scheduled, recurring basis
    - When incidents occur (bank robbery, customer assault, ATM theft, office building breach)
- Security measures, standards, or procedures put in place 3-years ago may not address today's threat landscape

THANK YOU!!

certified WBENC WOMEN'S BUSINESS ENTERPRISE

GMR 410 Trusted Advisors | Trusted Solutions

www.GMR410.com

GMR 410

Trusted Advisors | Trusted Solutions

certified WBENC WOMEN'S BUSINESS ENTERPRISE