Protecting Your Assets
- People and Property

presented by
Kevin Mellott, president
ERASE
Enterprises

Topics for Today

- The Vetting process- the difference between a background check and a background investigation
- CyberSecurity – the issue and the three primary attack methodologies
- Personal Safety Threats – responding to a confrontation and violent attacks

Before we begin -

- Remember, information is power and you lose that power when you give the information away
- Prevention is always the better approach than response, you just need to believe the need for the prevention efforts
- Deterrence is critical to security and safety
- Displacement may not stop the crime but it removes you as the potential victim

Background Check vs. Investigation

- A "check"
  - searches databases without establishing reliability and validity
  - is conducted via the Internet
  - information acquired is dated and very limited
- An "investigation"
  - validates and establishes reliability with all data sources including electronic research, interviews, multi-source comparison, and link matrix analysis
  - is as current as the level of effort involving field interviews and reviews of latest records

The Vetting Process

- In Texas the process of vetting is well regulated, make sure you are conducting a legal process
- Establish your budget for the process based on potential loss (reputation, financial, personal safety)

The Vetting Process

- You must understand the processes involved that produce the data you review
  - Bankruptcy court
    - Chapter 7
    - Chapter 11
    - Chapter 13
    - Filing date to Discharge date (range is important)
  - Criminal Court
    - Misdemeanor vs. Felony
    - Plea Bargain Agreements

The Vetting Process

- Validate all initial data on the subject of the process x 3 before beginning the check / investigation
- Repeat the process on all critical entities as people and business change over time and are influenced by occurrences in their life

CyberSecurity

- Primary Causes
  - Insider Action
    - Lack of Education
    - Disregard for policy or procedures
    - Error in judgment
  - External targeted or random attack
- Sources –
  - Business adversary
  - Personal antagonist
  - Current or ex-employee(s)
  - Criminal enterprise (including Software as a Criminal Service)
  - Hacktivist
  - Nation State

CyberSecurity

- Business Email Compromise
  - Attacker penetrates your computer system
    - Usually via a phishing attack or a targeted message
    - Social media mining and Spoofing are common
  - Attacker remains in system monitoring your activities learning your operations and personnel
  - Spoofed email is sent from C level officer or owner to CFO or authorized person to transfer funds
    - Supported by valid facts that induce receiver
    - Funds wired to bank account and moved quickly

CyberSecurity

- Ransomware Attacks
  - Attacker locks in on your computer from web site surfing and download activity
  - Attacker downloads Crypto Locker or similar encryption program to eliminate your access to data
  - Demands sent for "ransom" usually requested in Bit Coins and to be sent via the Dark Web
  - If paid, subsequent attacks are common
  - If not paid, your data may be lost permanently

CyberSecurity

- Man in the Middle Attacks
  - Often applied when you have a secured data system in place
  - Attackers monitor your inbound Internet traffic and select a vendor or routine source of communication
  - Attack is launched by spoofing email address of trusted source (vendor, outside advisor, etc.)
  - Code attached to spoofed email / document that allows access to your system for data theft

CyberSecurity

- Prevention Steps
  - Quality CyberSecurity Education for all personnel who have access to your data and internal systems
  - Implement Policy, Training, and Technology to stop penetrations including Black Listing Internet Sites that carry illicit code and are monitored by attackers
  - Follow Good CyberSecurity Hygiene practices
    - Strong passwords
    - Firewalls
    - Internet Security Suite Products that Work!

Personal Safety Threats

- Minimize your Desirability as a Target
  - Be aware of your surroundings and make sure the attackers know this fact
    - Stay off your phone
    - Walk in a directed fashion
    - Dress for the environment you are in
- Distract the Attacker
  - Throw purse or wallet down and away (pre-packaged)
  - High intensity light, pepper spray or throw object at face
- Draw them into YOUR fight zone
  - Never pursue them into their zone
  - Establish safe rooms at office and home
  - On the street take them to where you have the advantage

Personal Safety Threats

- Lethal Force
  - Before you plan to use this approach, consider the following
    - Understand the "wrongful death" law suit implications even if it is a justifiable action
      - Financial
      - Reputation harm
    - You must be very well trained, CHL / LTC training is NOT well trained
    - You must be physically and mentally prepared to take a life at all times
    - Your equipment must fit your lifestyle or you will not be consistent in your preparation

Questions?

Kevin Mellott

kevin@erase.com

214-679-1255 cell

ERASE Enterprises
1820 Preston Park Boulevard
Suite 1650
Plano, Texas 75093
214-501-5175