Jarron Bailey

Physical Security Assignment

Table of Contents

Facility location in dangerous locations

There exist a relationship pertaining to the type of business/organization and levels of risk. The location of the business can either positively or negatively affect the crime rate. Placing any facility in a high crime area will require rigorous safety procedures as opposed to placing the facility in a lethargic rural area. Several factors may attribute to the likelihood of crime such as:

- Rate of crime in the neighborhood
- Types of crime most commonly committed
- Number of people with access to your facility
- Whether your space is shared with other organizations
- Number of entrances and exits to your facility
- Insecure entrances or exits
- Lack of monitoring systems
- Lack of personnel

Overview

As of 2019, Tijuana, Mexico is reported at level two by the U.S Department of State Travel Advisory which advises travelers to exercise increased caution due to crime. Tijuana is home to 1.6 million inhabitants with a major crime problem.

Types of crime most commonly committed

Pickpocketing is highly prevalent in large crowd settings such as public transportation and tourist attractions. Pickpocktters select their target based on an assessment of vulnerability, prosperity, and inattention.

Violence in Tijuana is primarily constrained to the outskirts and not prevalent in the tourist areas. Tijuana Tourism Police tend to saturate the tourist areas in the aftermath of an incident and maintain a consistent presence in areas essential to tourists to maintain order.

Transnational Criminal Organizations (TCOs) are involved in narco-trafficking and human smuggling. Three rival cartels are battling for control of Baja California criminal operations the Sinaloa Cartel, the Cartel Jalisco Nueva Generación (CJNG), and remnants of the Arellano Félix Organization (AFO). Crime stemming from TCOs is primarily targeted and involved small criminal cells. After Sinaloa leader Joaquín “El Chapo” Guzmán’s arrest, narco related crimes spiked resulting in an unprecedented 3,150 homicides in 2018 in Baja California, with Tijuana holding 2,516 of those homicides.

AS of 2019, there is no current evidence of any transnational terrorist residing in this region, there is minimal risk to terrorism in Tijuana.

Physical securing a facility

Interlocking doors and access control solutions

Tend to be more prevalent for commercial and public buildings such as airports, schools, and government buildings. Interlocking doors exponentially increases complexity as additional doors, senors, and/or connecting rooms are added. Access control mechanisms can include card access, pin access, biometrics, etc. working in conjunction with the interlocking doors to ensure safety protocols. Also, mantraps door systems

can be used to help the control of people's inflow. Mantraps are usually powered open and closed with a built-in delay and safety sensors to help control traffic inflow.

Guards

Depending on the type of facility, guards may be necessary to provide protection for business operations, employees, and customers. Weaponized guards may be used to deter criminal activity from taking place in the facility or quickly access potential threats that may have bypassed initial security screens.

Protecting confidential information

As a business or organization keeping confidential information stored securely is a must, the information should be kept in a safe of a locking mechanism of some sort to ensure protection from possible intrusions.

Conclusion

A facility in Tijuana, Mexico may not be a target for the major criminal activities that take places such as the TCOs narco activities or the pickpocketing that affects tourists. However, to ensure maximum security an organization will need to consider using interlocking doors and access control solutions, mantraps, guards, and safes to attempt to maximize protection.

Sources

https://www.osac.gov/Content/Report/72d11598-3cfa-4ff4-a9bc-15f4aec22ce4
https://isotecsecurity.com/physical-security-risk-assessment-on-your-business/
https://isotecsecurity.com/interlocking-doors/

Facility security

How does one secure an HVAC system that has Internet of Things (IoT) capabilities?

Overview

An HVAC system is an abbreviation heating, ventilation, and air conditioning system. An HVAC system having Internet of Things capabilities is no different than a security camera, smart lock, or a smart doorbell. Each possesses the ability to transmit data via the internet which enhances there features and delivers a high magnitude of convenience into our lives. However, since these devices are internet-connected, they can serve as additional access points for cybercriminals.

How to secure IoT devices on a home network

1. **Give the router a name**
   Default names provided by the manufacturer often reveal the make and model of a particular device. Change the name helps reveal less information a cybercriminal can use against you.

2. **Use a strong encryption method for Router** When setting up wi-fi network access it is important to use WPA2 to help ensure network traffic is secure, as opposed to an encryption method like WPA which can be cracked very easily.

3. **Get rid of default passwords**
   Default passwords are one of the most commonly exploited vulnerabilities pertaining to IoT devices. To mitigate this vulnerability it is important to change default passwords and uses best practices when creating new passwords. The current best practice is to enforce a password at least 12 characters long with a mix of upper-cased, lower-cased, numbers, and symbols. Each IoT devices should get their password that should be changed at least every three months. Also if possible, adding layers of authentication is such a multi-factor authentication. A password manager is a convenient way to manage passwords for multiple accounts/devices.

4. **Create a segmented network topology**
   The IoT devices must live in a separate network, isolated from sensitive information that may live in computers or cellular devices. There is more than one way to achieve this network setup. The first option is to use your current router guest network capabilities, if and only if, it allocates network traffic into a different subnet. The second option is to obtain a second router, connect it to the internet gateway, and routes all IoT network traffic through the second router. The optimal router is one that supports a paid VPN service that also supports the DD-WRT Open VPN specification or L2TP/IPsec specification.

5. **Always keep devices updated**
   Make a habit to keep router firmware and IoT devices firmware and applications up to date. Many updates contain security patches that make the device more secure to mitigate potential exploiting.

Conclusion

Securing an IoT device on a home network is not a step solution, several procedures need to takes place such as using a strong encryption method for the router, using strong passwords for each device, and created a segmented network topology to ensure IoT is securely placed with a home network.

---

https://www.gadgetguy.com.au/five-steps-to-secure-your-iot-home-network-you-need-to/?display=all
https://us.norton.com/internetsecurity-iot-smart-home-security-core.html

What Risk Management Framework (RMF) requirements should one use to store media, protect media, and degauss/erase media?

The actions od storing media, protecting media, and degaussing/erasing media all fall under manipulating media. This falls under the National Institute of Standards and Technology(NIST) Special Publication 800-53 (Rev. 4) Media Protection Control Family. MP-2 (Media access) refers to Media access control, MP-4 (Media storage) refers to media storage controls, and MP-8 (Media Downgrading) refers to degaussing/erasing media.

How do you implement strong authentication?

Strong authentication is a blending of two different authentication methods to increase the safety of verifying identity. Passwords alone are not effective to protect accounts. Strong authentication is implemented when the users provide something that only the user has and input something only the user knows. Credit cards implement strong authentication all the time. A consumer uses the physical credit card(something that only

the user has) and the pin(something only the user knows), this is done to narrow chances of invalid credit card purchases.

Are there open-source possibilities?

There is an opensource implementation of strong authentication, one solution is LinOTP which offers enterprise-level to factor authentication with a new push token, offline one-time password authentication solution out of the box.

What are the problems associated with the implementation of strong authentication into facilities?

Multifactor authentication requires time and education for an organization or facility to properly enforces it. There are obvious advantages of multifactor, but there are disadvantages as well such as:

- The cost associated with the multifactor authentication setup rather than its hardware tokens, software tokens, etc.
- With some multifactor authentication implementations, if you lose the token aspect of it, you can be permanently locked out of the account which results in a loss of data
- Apart from the hardware or software cost of multifactor authentication, there is also a support cost associated with the technology

Sources

https://www.techopedia.com/definition/23939/strong-authentication
https://www.linotp.org/
https://cyberpulse.info/pros-and-cons-of-two-factor-authentication/
https://nvd.nist.gov/800-53/Rev4/family/Media%20Protection

Intelligence, Surveillance, and Reconnaissance (ISR)

Provide at least 300 words regarding the ethical considerations of using drones in physical security.

Link: https://www.youtube.com/watch?v=mpzk7OdbjBw

The ethicality and morality of the situations pertaining to drone usage all go back to the motives of the people behind the drone. A drone is just a tool used to aid the motives of the user controlling it. Therefore when we look at the U.S. and analyze the decisions that it has made around its drone usage, we have to discern if the drone is used is for the greater good. They are key problems revolving around drone usage including privacy and safety of those under surveillance. When we look at places like Iraq and Afghanistan who are under constant salience, we have to think about how the inhabitants of the land feel. The people must feel as if their rights are being stripped away from a foreign militant presence. Coupling the surveillance with drone strikes killing innocent people, ripping families apart. The drone is often sold as an effective weapon used to mitigate unwanted casualties. However, from the video, we can discern that using drones does keep U.S. clear from any harm, yet punishes local civilians in these areas. The drone is used to illuminate people of "fit" a certain profile that may be a possible threat. The issue of ethics comes into when discussing how much power should a foreign country have over another. The people of the target lands are living in turmoil because of the constant survivance and fear of death from a drone bomb strike. This injust can

become deeply rooted in their culture and heritage for the next generations. This results in a revolt or uprising where the U.S. becomes the target malicious attacks because the drone victims think their retaliation is justified. Are the Iraqis and Afghanistanis such a low-level people that it does not matter if many innocent people die in the process of killing one "potential" criminal. From a humane aspect, it is unfair and unjust.

Provide 300 words regarding drones are not only used for war but use of drones domestically. You also have the ability to discuss the use of the Unmanned Ground Vehicle (UGV) created by iRobot and its applications to physical security.

Link: https://www.youtube.com/watch?v=msHJLwYWX30

An unmanned ground vehicle is a vehicle that operates while being located on the ground without the presence of a human is not necessary. UGVs are ideal for any situation where humans would be placed in a very inconvenient, dangerous, or humanly impossible situation. The UGVs are equipped with a variety of different sensors used to gather intel about the surrounding environment. The UGVs will either autonomously make decisions or transport the intel back to a human operator who would then control the device through teleoperation. The design of UGVs features a core set of components such as platform, control systems, guidance interface, connection links, sensors, and system integration features. A fully autonomous UGVs may possess the ability to: collect detailed intel about a particular environment, as well as the interior of buildings; discern between objects, detecting humans or vehicles; navigate between waypoints without a human presence; intelligently avoid situations that may be harmful to humans, property, or itself; disarm, and/or remove explosives; and repair itself. The robots may also possess the ability to learn autonomously which includes the ability to: adapt to the surrounding environment; adjust its plan of execution based on the environment; learn new skills, and develop a sense of what's right or wrong depending on the mission at stake. Ues cases for this technology include peacekeeping operations, ground surveillance, gatekeeper/checkpoint operations, and rescue and recovery mission. Other applications include:

- Space
  NASA's Mars Exploration Rover project included two UGVs named Spirit and Opportunity. Spirit got trapped in a sand storm, and Opportunity has been in operation 12 years beyond its intended three-month lifespan. Curiosity landed Mars in 2011 with a mission objective of two years but has now been extended indefinitely.
- Agriculture Unmanned harvesting factors can help tackle short windows for optimal harvesting. They can also be used to monitor the health of livestock and crops.
- Mining UGVs can use its radar, visualization sensors, and lasers to traverse and map mine tunnels.
- Emergency response UGVs can be used in search and rescue, nuclear response, and fire fighting. These are a common condition that put humans at risk, but UGVs can help relieve these common dangerous acts.

Sources

https://www.hisour.com/unmanned-ground-vehicle-43142/

Biometrics

What is the importance of the Crossover Error Rate (CER)?

Authentication algorithms have the responsibility of simultaneously minimizing the permeability to intruders, and maximize the comfort level. To achieve this feat, they to exhibit both demanding and permissive behavior. This contradiction is the baseline for optimization in authentication algorithms. The measures of success and usability for the overall precision are the Crossover Error Rate (CER), which the key metric that identifies the threshold where False Acceptance Rate and False Rejection Rate are equal.

How can a small or midsize corporation implement the use of biometrics in their organization?

Commercially there are many biometric technologies available. The most common form of biometric technologies is fingerprint scanners and hand geometry scanners. Businesses may use laptops accompanied by fingerprint scanners. Today companies are offering enterprise laptops with fingerprint scanning technology built-in.

Fingerprint scanners

Fingerprint scanners are consistently constructed to be small and portable, which makes them ideal for desk usage. They are ideal for single-user identification. They are extremely affordable; however, the fingerprint scanners aren't usually suitable for more than 100 users. fingerprint scanners are also sold as pluggable USB devices that can attach to keyboards or mice. Also, fingerprint scanners can be used for physical security by integrating storage devices.

Hand geometry scanners

Hand geometry scanners are more expensive than fingerprint scanners and take up additional space. However, hand scanners support a larger amount of people. Hand geometry readers are generally used for physical security.

Retina and Iris scanners

The expense of deploying iris and retina scanners are ideal unless the location requires very high security. The retina and iris scanners may ring between $2,000 and $10,000. Despite the cost, they exhibit the highest accuracy amongst the commercial-grade biometric security products.

Conclusion

When deciding to integrate biometric technologies within an organization, you have to consider several things such as do the benefits outweigh the cost. The most optimal solutions for small to mid-size companies will either be fingerprint scanners or hand geometry scanners. Fingerprint scanners are the cheap and most versatile solution to securing laptops and storage devices.

Should strong authentication be implemented for the use of biometrics?

I believe strong authentication should be implemented with biometrics. Biometrics are additional layers of security wit low error rates. For example, fingerprint scanners exhibit 1% to 3% error rates. Given the low error rate, I think any additional layer of security is great.

Why are American citizens reluctant to the use of biometrics?

Americans citizens may be reluctant to use biometrics because of the personal nature of identification. Users are required to share personal information which is stored digitally. The risks of not safely securing this private information increases. Americans are used to free speech and privacy, having biometrics stored may cause people as if their privacy is being invaded.

Sources

https://www.igi-global.com/dictionary/behavioral-based-technologies-for-enhancement-of-loginpassword-systems/6294
https://www.allbusiness.com/is-biometric-security-right-for-your-business-8518533-1.html