2.4 Assignment: Threat Analysis (Phase 1 of Final Project)

Company Name: Safeguard

Professor: Joseph Snider

11 Group Project

Name: Neha Pramida Peddhi – 2823945

Sukrutha Vennam- 2638180

Sai kumar Bathula – 2825243

Venkata Keerthi Inganti – 2822554

Sravanthi Arava – 2638897

Shivani Komaravelli – 2640897

Divya Komarthi – 2638271

Anam Bijal - 2823484

Syed Abdullah Hussain – 2824790

Khaja Faheem Uddin – 2824913

Abdul Samad Sohail – 2823700

4 a)

**Executive Summary:**

Safeguard Systems is a top supplier of complete security systems for commercial and residential buildings. Modern security systems are the company's area of expertise, and they are designed, installed, and maintained to safeguard clients' assets and workers.

Businesses and homeowners are increasingly looking for trustworthy and cutting-edge security solutions due to the growing concerns of criminal activity, theft, and unwanted entry. Monitoring cameras, access control systems, intrusion detection systems, and alarm monitoring services are just a few of the goods and services that Safeguard Systems provides. These solutions are made specifically for each client, taking into account aspects like location, size, and particular security issues.

The business has a staff of highly qualified experts with years of security industry experience. To stay on the cutting edge of technical breakthroughs, Safeguard Systems makes research and development investments. They offer cutting-edge security products that are renowned for their exceptional performance, dependability, and scalability by collaborating with top manufacturers.

Safeguard Systems places a high premium on customer satisfaction. They provide thorough consulting services to evaluate security requirements, create unique solutions, and offer ongoing support and maintenance. A committed customer support team is on call around-the-clock to immediately respond to any worries or challenges.

Commercial buildings, retail stores, educational institutions, healthcare facilities, and apartment complexes are just a few of the sectors that Safeguard Systems has successfully served. A strong reputation, a devoted customer base, and favorable recommendations are the results of the company's dedication to excellence.

Safeguard Systems continues to adapt and innovate in a constantly changing security landscape. They research cutting-edge technologies to improve the effectiveness and efficiency of their security systems, including artificial intelligence, machine learning, and cloud-based options.

Safeguard Systems is devoted to sustaining the greatest levels of excellence, professionalism, and honesty as they grow their business and investigate new markets. Through cutting-edge security systems that provide great performance and dependability, the company is dedicated to bringing clients peace of mind and safeguarding their assets.

b)  
**Threat Analysis: Safeguard Systems**

**Introduction:**

The purpose of this threat analysis is to identify potential threats to Safeguard Systems and assess their likelihood and potential impact. By conducting a comprehensive analysis, Safeguard Systems can develop strategies to mitigate these threats and enhance the overall security of their operations.

**Methodology:**

The threat analysis was conducted using a combination of primary and secondary research.

Primary research involved interviews with industry experts and key stakeholders within Safeguard Systems.

Secondary research included reviewing industry reports, security guidelines, and relevant literature. The findings were analyzed to identify potential threats and assess their significance.

**Threat Identification:**

**Physical Threats:**

* Unauthorized entry into buildings, theft of security instruments, and theft of priceless valuables are all examples of crime and theft.
* Criminal activity and violence, on the other hand, refers to the intentional destruction of security infrastructure such access control systems and CCTV cameras.
* Unauthorized access is when someone enters a secured location without authorization or abuses with security measures.



**Cybersecurity Threats:**

* Criminals are trying to compromise the network security of Safeguard Systems in order to access confidential information without authorization.
* Introduction of dangerous software or attacks containing ransomware that may interfere with operations or danger data integrity are referred to as viruses and ransomware, respectively.
* Attacks using social engineering: Influencing workers to reveal private information or allow unwanted access.



**Technological Threats:**

* Problems with equipment or breakdowns that can leave security coverage gaps are known as system failures.
* Interruptions in the channels of communication between security devices and monitoring systems.
* Problems remain unprotected because security systems are not constantly updated with the newest firmware and software updates.



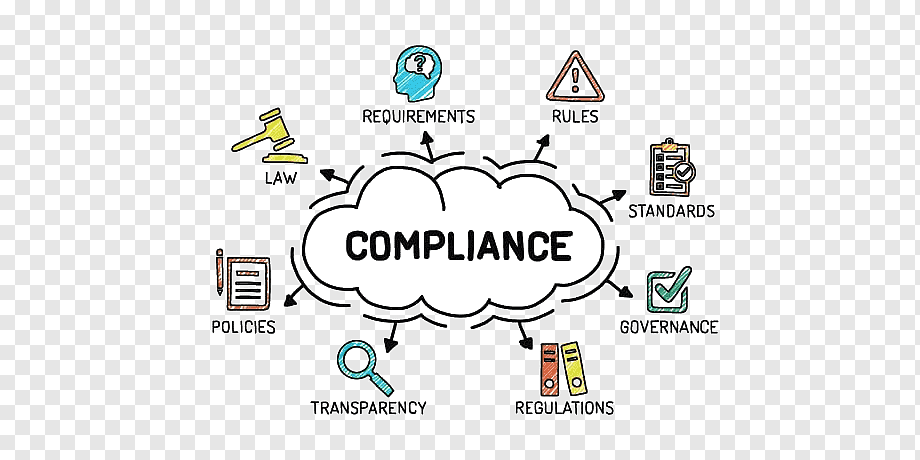
**Environmental Threats:**

* Floods, earthquakes, and fires are examples of natural disasters that can harm infrastructure and compromise security measures.
* Loss of electrical power that may affect how well security and surveillance equipment functions.



**Regulatory and Compliance Threats:**

* Improvements to current security and privacy laws need for the updating of Safeguard Systems procedures and infrastructure.
* Failure to comply with regulations can result in fines, damage to one's reputation, and lost commercial possibilities.



**Threat Assessment:**

The possibility and potential impact of each discovered attack on Safeguard Systems were evaluated. Each threat was ranked according to its seriousness using a qualitative scale that took into account aspects like historical data, market trends, and expert opinions.

**Risk Mitigation Strategies:**

* To reduce potential dangers and weaknesses, different methods for risk reduction were created for each threat that was discovered.
* These methods consist of placing into operation thorough access control systems and security cameras to stop and catch theft and unlawful access.
* fixing software weaknesses by routinely patching and updating security systems.
* implementing consistent training and awareness campaigns to inform staff about cyberthreats and social engineering attacks.
* To reduce the effects of system breakdowns and data breaches, disaster recovery and backup procedures must be put into place.
* Setting up robust physical security measures, such as perimeter protection, security guards, and alarms, to thwart sabotage and damage.
* By conducting routine audits and evaluations, compliance with pertinent security and privacy standards is ensured.

**Implementation Plan:**

To help with the execution of the risk reduction techniques, an implementation plan was created. Assignment of duties, deadline setting, and resource allocation are all part of the plan. Additionally, it takes into account any difficulties or restrictions that can emerge during the implementation procedure.

**Monitoring and Review:**

A monitoring and review procedure was set up to keep tabs on how well the risk mitigation methods that were put into place were working. Indicators and metrics were established to gauge the effectiveness of the measures and spot any new risks or shifts in the risk environment. To make sure the threat analysis is current and pertinent, regular reviews will be done.

**Conclusion:**

Safeguard Systems may strengthen its entire security posture and protect its operations, assets, and clients by completing a thorough threat analysis and putting into place efficient risk mitigation techniques. The success of these measures will be continuously monitored and reviewed, allowing for proactive adjustments to handle new threats.

C)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat Category** | **Potential Threats** | **Likelihood** | **Potential Impact** | **Risk level** | **Risk Mitigation Strategies** |
| Physical Threats | Burglary and Theft | High | High | Medium-High | Install access control systems, surveillance cameras, and alarms. Regularly review and update security protocols. |
|  | Vandalism and Sabotage | Medium | Medium | Medium | Implement robust perimeter protection measures. Conduct regular inspections of security infrastructure. |
|  | Unauthorized Access | Low | High | Medium | Perform background checks on employees and contractors. |
| Cybersecurity | Hacking and Data Breaches | Medium | High | Medium-High | Implement strong authentication and encryption measures. Regularly update and patch software and systems. |
|  | Threats Malware and Ransomware | Medium | Medium-High | Medium | Conduct regular security audits and penetration testing. |
|  | Social Engineering Attacks | Low | Medium | Low-Medium | Provide cybersecurity awareness training to employees. |
| Technological | System Failures | Medium | Medium - High | Medium | Implement redundant systems and backup solutions. Regularly maintain and update security devices. |
| Threats | Communication Failures | Low | Medium | Low-Medium | Establish backup communication channels and protocols. |
|  | Lack Of System Updates | Low | Low | Low | Ensure timely software and firmware updates. |
| Environmental | Natural Disasters | Low | High | Low - Medium | Develop disaster recovery plans and backup power solutions. |
| Threats | Power Outages | Medium | Medium | Medium | Regularly test backup power systems and protocols. |
| Regulatory | Changes In Regulations | Medium | Medium | Medium | Stay updated on security and privacy regulations. Develop processes for adapting to regulatory changes. |
| Compliance Threats | Non-compliance | Low | High | Medium-High | Conduct regular compliance audits and assessments. |

References:

* Executive summary – safeguard system - <https://nces.ed.gov/pubs98/safetech/execsum.asp>
* <https://www.sciencedirect.com/topics/computer-science/threat-analysis>
* Federal Bureau of Investigation. (2022). Cybersecurity Best Practices for Businesses -

<https://www.fbi.gov/investigate/cyber>

* <https://www.gov.mb.ca/health/phia/docs/security_safeguards.pdf>