**SILVER STAR MINES – CASE STUDY**

A case study involving the operations of a fictional company Silver Star Mines illustrates this risk assessment process. Silver Star Mines is the local operations of a large global mining company. It has a large IT infrastructure used by numerous business areas. Its network includes a variety of servers, executing a range of application software typical of organizations of its size. It also uses applications that are far less common, some of which directly relate to the health and safety of those working in the mine. Many of these systems used to be isolated, with no network connections among them. In recent years, they have been integrated and connected to the company’s intranet to provide better management capabilities. However, this means they are now potentially accessible from the Internet, which has greatly increased the risks to these systems.

A security analyst was contracted to provide an initial review of the company’s risk profile and to recommend further action for improvement. Following initial discussion with company management, a decision was made to adopt a combined approach to security management. This requires the adoption of suitable baselines standards by the company’s IT support group for their systems. Meanwhile, the analyst was asked to conduct a preliminary formal assessment of the key IT systems to identify those most at risk, which management could then consider for treatment.

The first step was to determine the **context for the risk assessment**. Being in the **mining industry sector places the company at the less risky end of the spectrum, and consequently less likely to be specifically targeted. Silver Star Mines is part of a large organization and hence is subject to legal requirements for occupational health and safety and is answerable to its shareholders**. Thus, **management decided that it wished to accept only moderate or lower risks in general**. The **boundaries for this risk assessment were specified to include only the systems under the direct control of the Silver Star Mines operations. This excluded the wider company intranet, its central servers, and its Internet gateway**. This assessment is sponsored by Silver Star’s IT and engineering managers, with results to be reported to the company board. The assessment would use the process and ratings described in this chapter.

Next, the key assets had to be identified. The analyst conducted interviews with key IT and engineering managers in the company. Several the engineering managers emphasized how important **the reliability of the SCADA network and nodes were to the company. They control and monitor the core mining operations of the company and enable it to operate safely and efficiently and, most crucially, to generate revenue**. Some of these systems also maintain the records required by law, which are regularly inspected by the government agencies responsible for the mining industry. Any failure to create, preserve, and produce on demand these records would expose the company to fines and other legal sanctions. Hence, these systems were listed as the first key asset.

Several the IT managers indicated that a large amount of **critical data was stored on various file servers either in individual files or in databases. They identified the importance of the integrity of these data to the company**. Some of these data were generated automatically by applications. Other data were created by employees using common office applications. Some of this needed to be available for audits by government agencies. There were also data on production and operational results, contracts and tendering, personnel, application backups, operational and capital expenditure, mine survey and planning, and exploratory drilling. Collectively, the integrity of stored data was identified as the second key asset.

These managers also indicated that three key systems—the **Financial, Procurement, and Maintenance / Production servers—were critical to the effective operation of core business areas. Any compromise in the availability or integrity of these systems would impact the company’s ability to operate effectively**. Hence each of these were identified as a key asset.

Lastly, the analyst identified e-mail as a key asset, because of interviews with all business areas of the company. The use of e-mail as a business tool cuts across all business areas. Around 60% of all correspondence is in the form of e-mail, which is used to communicate daily with head office, other business units, suppliers, and contractors, as well as to conduct a large amount of internal correspondence. **E-mail is given greater importance than usual due to the remote location of the company. Hence the collective availability, integrity, and confidentiality of mail services was listed as a key asset**.

Having determined the list of key assets, the analyst needed to identify significant threats to these assets and to specify the likelihood and consequence values. **The major concern with the SCADA asset is unauthorized compromise of nodes by an external source**. These systems were originally designed for use on physically isolated and trusted networks and hence were not hardened against external attack to the degree that modern systems can be. Often these systems are running older releases of operating systems with known insecurities. Many of these systems have not been patched or upgraded because the key applications they run have not been updated or validated to run on newer OS versions. More recently, the SCADA networks have been connected to the company’s intranet to provide improved management and monitoring capabilities. Recognizing that the SCADA nodes are very likely insecure, these connections are isolated from the company intranet by additional **firewall and proxy server systems**. Any external attack would have to break through the router company firewall, the SCADA network firewall, and these proxy servers to attack the SCADA nodes. This would require a series of security breaches. Nonetheless, given that the various computer crime surveys suggest that externally sourced attacks are increasing and known cases of attacks on SCADA networks exist, the analyst concluded that while an **attack was very unlikely, it could still occur**. The consequence of the SCADA network suffering a successful attack was discussed with the mining engineers. They indicated that **interference with the control system could have serious consequences as it could affect the safety of personnel in the mine. Ventilation, bulk cooling, fire protection, hoisting of personnel and materials, and underground fill systems are possible areas whose compromise could lead to a fatality. Environmental damage could result from the spillage of highly toxic materials into nearby waterways. Additionally, the financial impact could be significant, as downtime is measured in tens of millions of dollars per hour**. There is even a possibility that Silver Star’s mining license might be suspended if the company was found to have breached its legal requirements.

The second asset concerned the integrity of stored information. The analyst noted **numerous reports of unauthorized use of file systems and databases in recent computer crime surveys**. These assets could be compromised by both internal and external sources. These can be either the result of intentional **malicious or fraudulent acts, or the unintentional deletion, modification, or disclosure of information**. All indications are that such database security breaches are increasing and that access to such data is a primary goal of intruders. These systems are located on the company intranet and hence are shielded by the company’s outer firewall from much external access. However, should that **firewall be compromised, or an attacker gain indirect access using infected internal systems, compromise of the data was possible. With respect to internal use, the company had policies on the input and handling of a range of data, especially that required for audit purposes**. The company also had policies on the backup of data from servers. However, the large number of systems used to create and store this data, both desktop and server, meant that overall compliance with these policies was unknown. Discussions with some of the company’s IT managers revealed that some of this information is **confidential and may cause financial harm if disclosed to others. There also may be substantial financial costs involved with recovering data and other activities after a breach. There is also the possibility of serious legal consequences if personal information was disclosed or if the results of statutory tests and process information were lost**.

The availability or integrity of the key Financial, Procurement, and Maintenance/Production systems could be compromised by any form of attack on the operating system or applications they use. Although their location on the **company intranet does provide some protection**, due to the nature of the company structure a number of these systems have not been patched or maintained for some time. **This means at least some of the systems would be vulnerable to a range of network attacks if accessible**. **Any failure of the company’s outer firewall to block any such attack could very likely result in compromise of some systems by automated attack scans.** These are known to occur very quickly, with several reports indicating that unpatched systems were compromised in less than 15 minutes after network connection. Hence a likelihood of Possible was specified. Discussions with management indicated that the degree of harm would be proportional to extent and duration of the attack. In most cases a rebuild of at least a portion of the system would be required, at considerable expense. False orders being issued to suppliers or the inability to issue orders would have a negative impact on the company’s reputation and could cause confusion and possible plant shutdowns. **Not being able to process personnel time sheets and utilize electronic funds transfer and unauthorized transfer of money would also affect the company’s reputation and possibly result in a financial loss.** The company indicated that the **Maintenance/Production system’s harm rating should be a little lower due the ability of the plant to continue to operate despite some compromise of the system. It would, however, have a detrimental impact on the efficiency of operations**.

The last asset is the **availability, integrity, and confidentiality of mail services**. Without an effective e-mail system, the company will operate with less efficiency. Several organizations have suffered failure of their e-mail systems because of mass e-mailed worms in past years. New exploits transferred using e-mail are reported. Those exploiting vulnerabilities in common applications are of major concern. The **heavy use of e-mail by the company, including the constant exchange and opening of e-mail attachments by employees, means the chance of compromise, especially by a zero-day exploit to a common document type, is very high**. While the company does filter mail in its **Internet gateway**, there is a high probability that a zero-day exploit would not be caught. A denial-of-service attack against the mail gateway is very hard to defend against. Hence a **likelihood rating of Almost Certain** was selected in recognition of the wide range of possible attacks and the high chance that one will occur sooner rather than later. Discussions with management indicated that while other possible modes of communication exist, they do not allow for transmission of electronic documents. The ability to obtain electronic quotes is a requirement that must be met to place an order in the purchasing system. Reports and other communications are regularly sent via this e-mail, and any inability to send or receive such reports might affect the company’s reputation. **There would also be financial costs and time needed to rebuild the e-mail system following a serious compromise**.

**Analysis**

**1. Given previous description of data collected from the Silver Star Mines, create a risk report filling the following table (use the class material to fill the table).**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Threat / Vulnerability | Existing Control | Likelihood | Consequence | Level of Risk | Risk Priority |
| Reliability and integrity of the SCADA nodes and network. | Unauthorized  modification of  control system | Layered  firewalls  and server | Rare | Major | High | 1 |
| Integrity of stored file and database information. | Corruption, theft,  loss of info | Firewall,  policies | Possible | Major | Extreme | 2 |
| Availability and integrity  of financial system. | Attacks/errors  affecting system | Firewall,  Policies | Possible | Moderate | High | 3 |
| Availability and integrity  of procurement system. | Attacks/errors  affecting system | Firewall, Policies | Possible | Moderate | High | 4 |
| Availability and integrity  of production system. | Attacks/errors  affecting system | Firewall, Policies | Possible | Minor | Medium | 5 |
| Availability and integrity  of mail servers. | Attacks/errors  affecting system | Firewall, and Mail Gateway | Almost Certain | Minor | High | 6 |

**2. Using the stakeholder risk appetite, provide your advice about the risk, suggesting measures to solve the question.**

The information was summarized and presented to management. All the resulting risk levels are above the acceptable minimum management specified as tolerable. Hence treatment is required. Even though the second asset listed had the highest level of risk, management decided that the risk to the SCADA network was unacceptable if there was any possibility of death, however remote. Additionally, the management decided that the government regulator would not look favorably upon a company that failed to highly rate the importance of a potential fatality. Consequently, the management decided to specify the risk to the SCADA as the highest priority for treatment. The risk to the integrity of stored information was next. The management also decided to place the risk to the e-mail systems last, behind the lower risk to the Maintenance/Production system, in part because its compromise would not affect the output of the mining and processing units and because treatment would involve the company’s mail gateway, which was outside the management’s control.

The result of this risk assessment process is shown in above Table, the resulting overall risk register table. It shows the identified assets with the threats to them, and the assigned ratings and priority. This information would then influence the selection of suitable treatments. Management decided the first five risks should be treated by implementing suitable controls, which would reduce either the likelihood or the consequence should these risks occur. None of these risks could be accepted or avoided. Responsibility for the final risk to the e-mail system was found to be primarily with the parent company’s IT group, which manages the external mail gateway. Hence the risk is shared with that group.