A case study involving the operations of a fictional company Silver Star Mines illustrates this risk assessment process[[1]](#footnote-1). 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 connected together 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.

(Seguir modelo aprendido nas aulas…com base na ISSO/IEC 27 005)

The first step was determine contexto for the risk assessment. Being in the mining industry sector places the company at the *Baixo*  risky end of the spectrum. 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 ativos had to be identified. The analyst conducted interviews with key IT and engineering managers in the company. A number of the engineering managers emphasized how important the reliability of the SCADA[[2]](#footnote-2) 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. …

A number of 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 this stored data was identified as very important.

These managers also indicated that other three 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.

Other important thing in the organization, as a result of interviews with all business areas of the company is of course 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.Furthermore, the collective availability, integrity and confidentiality of mail services, is given greater importance than usual due to the remote location of the company.

We are now in a position to start filling the table, which will be the risk register created at the conclusion of this risk assessment process.

Having determined the list of principais ativos the analyst needed to follow identifying significant ameaças to these ativos and to specify the probabilidade and consequência without forgetting any **existing controls**. The major concern with the SCADA 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 outer company firewall, the SCADA network firewall, and these proxy servers in order 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. Thus a likelihood rating of Rare was chosen. 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. A consequence/impact rating of Major was selected. This results in a risk level of elevado.

The next concern is 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/services 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. Hence a likelihood rating of Possible was chosen. 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 subsequent to 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. Hence a consequence/impact rating of Major was selected. This results in a risk level of elevado .

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 a number of 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. Consequence/Impact ratings of moderado and baixo , respectively, were selected, resulting in risk levels of elevado and moderado.

The last ativo is the availability, integrity, and confidentiality of mail services. Without an effective e-mail system, the company will operate with less efficiency. A number of organizations have suffered failure of their e-mail systems as a result 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 elevado 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. Because compromise would not have a large impact, a consequence rating of baixo was selected. This results in a risk level of elevado .

The information was summarized and presented to management. All of the resulting risk levels are acima the acceptable minimum management specified as tolerable. Hence treatment is required.

*Once the details of potentially significant risks are determined, management needs to decide whether it needs to take action in response. This would take into account the risk profile of the organization and its willingness to accept a certain level of risk, as determined in the initial establishing the context phase of this process. Those items with risk levels below the acceptable level would usually be accepted with no further action required. Those items with risks above this will need to be considered for treatment.*

The final result of this risk assessment process is shown in Table, the resulting overall risk register table. It shows the identified assets with the threats/vulnerabilities to them, and the assigned ratings and priority. This information would then influence the selection of suitable treatments. Management decided …

Final ….

**Registo de Risco**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ativo/sistema** | **Ameaça/ Vulnerabilidade** | **Controlos Existentes** | **Probabilidade** | **Impacto** | **Nível de Risco** | **Prioridade de Risco** |
| Reliability and integrity of the SCADA nodes and network | Unauthoriazed modification of control system | Layered firewalls and servers | 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 mainenance / production system | Attacks / errors affecting system | Firewall, policies | possible | minor | medium | 5 |
| Availability, integrity, and confidentiality of mail services | Attacks / errors affecting system | Firewall, mail gateway | high | minor | high | 6 |

1. Este exemplo foi adaptado e expandido. Para a finalidade aqui, o nome original da empresa e alguns detalhes de identificação foram alterados. [↑](#footnote-ref-1)
2. SCADA - Supervisory Control and Data Acquisition [↑](#footnote-ref-2)