HADMÉRNÖK

XII. Évfolyam 3. szám – 2017. szeptember

THE ROLE OF THE PROTECTION OF PRIVATE PROPERTY IN THE DAMAGE INVESTIGATION SYSTEM OF INDUSTRIAL-SIZED COMPANIES

AZ IPARI MÉRETŰ TÁRSASÁGOK KÁRESETI VIZSGÁLATI RENDSZERÉBEN, A MAGÁNTULAJDON VÉDELEM SZEREPE

KÁLMÁN, László

(ORCID: 0000-002-4724-5190)

l.kalman1972@gmail.com

Abstract

Protection strategy design, organisation, and sensitive issues of asset protection and of the internal investigation system at industrial facilities and manufacturing plants. The author presents a possible design and organisation of protection through the example of a large industrial manufacturer. What measures should be adopted in the interest of internal asset protection and security and with which organisational structure and tools can the protection of private assets be maintained at the most acceptable level. The author shall deal specifically with the structure and design of the internal protection organisation, offering replies to questions related to investigations systems and sensitive issues.

Keywords**:** *security organisation, protection strategy, risk assessment, evaluation*

Absztrakt

Ipari létesítmények, gyártó üzemek tulajdonvédelmének, belső vizsgálati rendszerének védelmi stratégiai tervezése szervezése, és azok szenzitív kérdései. A szerző bemutatja egy lehetséges védelmi tervezés, szervezés kialakítását egy nagyméretű ipari gyártó üzemen keresztül. A belső tulajdonvédelem és biztonság érdekében milyen intézkedéseket célszerű foganatosítani, milyen szervezeti felépítésben és milyen eszközökkel tudjuk a magántulajdon védelmét a lehető legelfogadhatóbb szinten tartani. Szerző kifejezetten a belső védelmi szervezet felépítésével és kialakításával, vizsgálati rendszerek kérdéseivel és szenzitív kérdések megválaszolásával foglalkozik.

Kulcsszavak: *biztonsági szervezet, védelmi stratégia, kockázatelemzés, értékelés*

A kézirat benyújtásának dátuma (Date of the submission): 2017.05.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.16.

INTRODUCTION

Today, it is an indispensable part of the efficient operation of manufacturing plants to create a protection system and strategy for both assets produced and other assets which best serve their safeguarding. In recent decades we have witnessed almost yearly changes in the area of asset protection. Principles developed previously in the subject of asset- and equipment protection have been analysed countless times in professional literature. General methods with varying degrees of applicability were proposed for these in an attempt to provide guarantees of protection.

Organisational measures represent a key element of complex protection strategies. In the present case, the protection strategy is only one part of the totality of these measures; therefore the creation of the protection strategy will be discussed as part of organisational measures. One thing is certain: this process has been changing and will continue to change due to both technical development and the evolution and increasing awareness of the profession. Naturally, we find unique features, since security technology, too,– as any multidisciplinary branch of science – requires constant change and adaptation in terms of the elaboration of protection strategies. The development and significance of organisational measures and of the elaboration of internal protection strategies have been changing continuously throughout history, generally in line with developments in government structures, legislation, and market situations. Today, however, there is greater demand not only for efficiency, but also for safeguarding property. Let us examine how asset protection and protection strategy can assist the activities and investigation system of companies and manufacturing plants at an industrial-sized organisation, as part of asset security. Over the years, outsourcing, which started at the time of the change to a democratic regime, and the outbreak of the economic crisis have increasingly forced out the operation of own-employed security. Mixed protection methods, such as a private security force, reception service, armed civilian guards, and their combined application already existed decades ago, not only now.

Following the change to a democratic regime, upon the recommendation of the Ministries of Industry the protection of private property was "outsourced" to mostly privately owned companies, which provided protection of the object. Based on practical experience we can say that external companies rarely play an investigative role at large industrial facilities. This task remained largely within the competence of the managers and persons with the rights of the employer working there, thus asset protection was aimed at protecting the object, largely against external intrusion, as well as detecting certain incidents of theft by employees. Today, we know full well that private asset protection organisations providing security and asset protection activities can have a much greater role than this in protection. It is not likely that larger companies would wish to hand over their internal investigation system to an outside party. This is a very rare, and also area-dependent case; though it is considered a highly modern approach. Here, I will deal with the options of creating the internal protection system of own-employed asset protection services within organisations. We now see that own protection will gain ground on the market in the future, thanks to the increasingly conscious organisation of protection, which will contribute to and increase lawful employment, together with significant savings. The general comparison between investigative methods and scientific studies is based on empirical methods and observations, using analysis and synthesis. Through these methods I will strive to create a potential modern protection strategy and also touch upon ways to structure the overall security organisation, highlighting its complexity.

Objective

Before we create our strategy or plan, we need to review the nature of the property to be protected, the direction from which it faces the highest risk of threat, and the elements that can damage it. Asset protection usually employs maximum force against outside intrusion, violent events, and burglary. Technical equipment and options - mainly camera and intrusion alarm systems, sensors, and mechanical protective equipment – are usually deployed in line with this strategy. Despite this, it has been proven countless times that damage caused internally is much greater in its extent, yet protection against it is, surprisingly, far less extensive than protection directed outwards. Naturally, this does not mean that we should neglect the implementation of outdoor protection.

The creation of asset protection security has complex interpretations, based on various branches of science. Practical experience, however, shows that the outer circle of protection is usually given more emphasis in the deployment of technical equipment. So how should we set up our internal protection system, and against what? The most important is to define first what extraordinary events may occur due to external and internal risks. With regard to external events, the malicious external intent may take the form of unlawful appropriation, vandalism, sabotage, and in some cases even industrial espionage. But what threatens us from the inside? First, we must accept as our basis something that is common knowledge in our profession; namely that unlawful possession and theft attempts by employees are well-known damage events at companies. We defend against this through inspections at both exit from and entry to the workplace, since we must also prevent equipment that can be used for committing unlawful appropriation or may harm and reduce the utilisation of working hours being brought onto the site of our company. Another major branch of damage events concerns events caused intentionally or through negligence by employees or by technical equipment, sudden accidents, disasters, or other extraordinary events. Naturally, commensurate protection must be developed through the combined effect of all infrastructural elements (electronic devices: cameras, access control, alarm systems, etc.) and organisational measures that are part of our complex protection strategy. [1]”Personal- and asset protection is, therefore, a changing, dynamic state, which is directly influenced by two factors. One of these is the threat, the other the protective resources used.” [2 p 6]

Indirectly, there are of course other factors that play a role, but the ones mentioned above are those with a direct impact on security. In the present case, I will examine specifically the organisation and investigative method of internal investigations in connection with damage events and disciplinary cases. Which method and the combination of which organisations can minimise damage within the company?

The organisation itself, which consists of all participants of the protection organisation, which may include the fire prevention, security technology, machine safety, health protection, civil protection, and asset protection organisations, is in itself insufficient for maximising protection. It is also necessary to support, inform, and train the managers who exercise the rights of the employer, as to how they could take part in protecting company assets. In addition, it is also vital to inform and train workers and employees in order to protect company assets, since as the old slogans already used to say, protecting the assets of a company or organisation is the duty of every employee and the responsibility of every manager. This means that no matter how well-trained individual organisations are, they can only provide efficient and complex protection and prevention through total cooperation.

A possible setup for security organisation

Regarding the setup of security organisations I would like to present one option for its structure through an organisational diagram. We need to take into account the actual size and divisions of the organisation, which naturally depend on the industrial sector and the activity.

The structure of the security organisation is also influenced by the extent and nature of risks. Nonetheless, certain relations exist, which can provide a model of a suitable structure for all organisations. The security organisation outlined below, presenting the branches involved in security, is applicable to particularly large industrial environments.

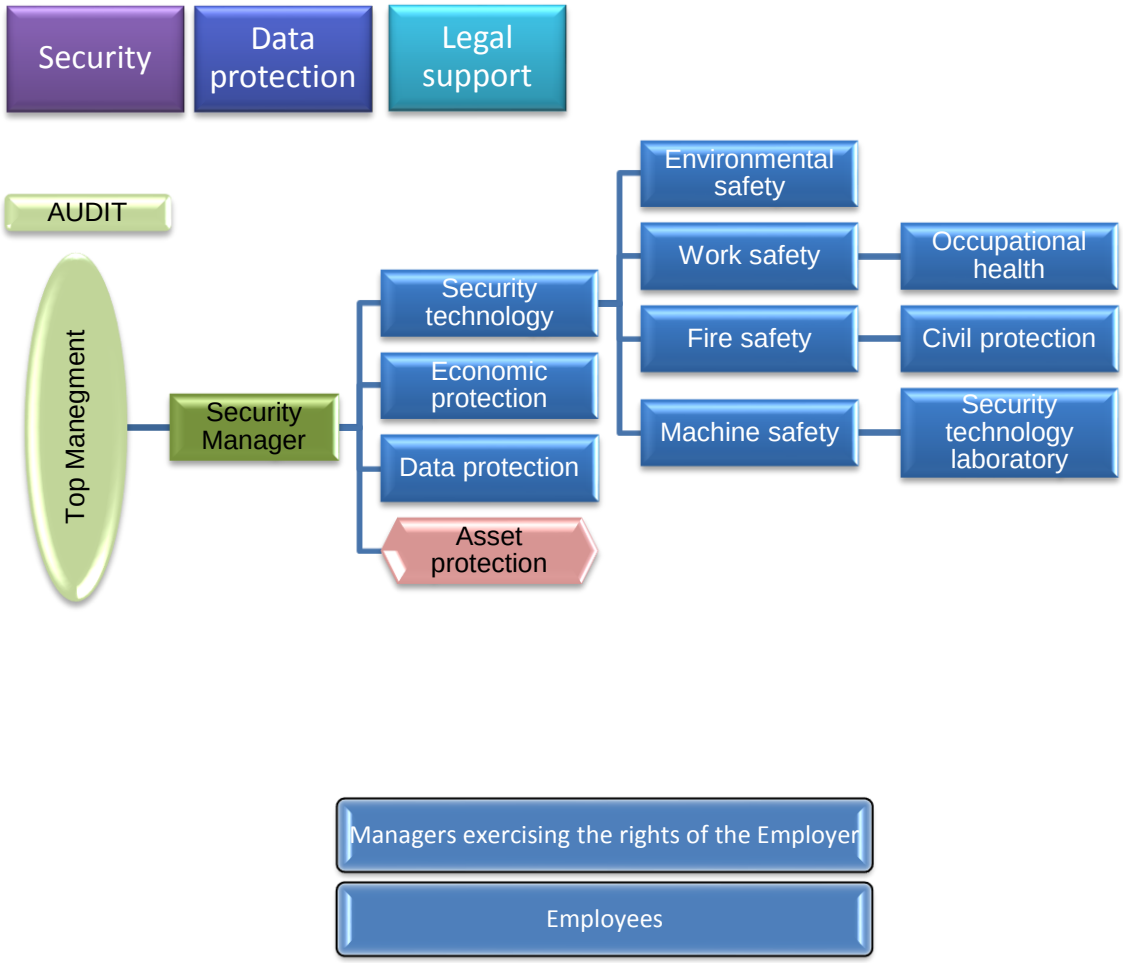

Figure 1 Security organisations (Author: L. Kálmán)

The figure above clearly shows the hierarchical structure of security organisations, which may vary in its form depending on the organisation. If the size of the organisation does not call for separate branches, a single organisation may fulfil several roles. The basic pillar of the operational efficiency of a security organisation is that it must be independent and not subordinated to any other organisation not directly involved in security. In case of subordination the security activity can no longer be carried out independently and professional representation will be inadequate. Unfortunately, I have come across numerous cases of subordination, which does not facilitate correct operation and weakens the integrity of the security organisation. Controlling organisations generate conflicts; therefore it is very important to establish the right objective and strategy, which enable the management of conflicts and ensure security awareness. The correctly drafted administrative controls must be unambiguous and clear. Data from the survey on fraud by the Association of Certified Fraud Examiners (ACFE) in 2010 were reflected in several Hungarian presentations, conferences, and studies. In his essay entitled “Signs of corruption in procurement processes” Gábor Amon also summarised the direct and indirect signs of corruption within organisations. [3]

Procurement and investment processes require even greater caution not only with regard to their operation, but also in terms of the regulation of their control processes. Several international surveys substantiate abuses and opportunities for such in the above areas. In her work entitled "Professional scepticism in auditing – the relation between fraud detection and professional scepticism", which is based on international studies on auditing, Krisztina Veit studies these relations and models in depth in light of the results of surveys by international organisations. Her work gives us proper insight into auditing and related audits. [4]

With regard to procurement and investments a clear correspondence can be set up between investigative bodies and the above figure. Economic protection includes the auditor and their organisation, accounting and financial participants, the persons who directly control and monitor procurement and investment processes and their internal and external players. Audits can play a part either directly in the investigation or independently of that. The essence of audits is to examine compliance with prescribed criteria through the compilation and objective evaluation of "evidence" and facts. Audits may be comprehensive, in which case every relevant requirement and rule is examined, or partial, targeting a specific area. (production process audit, administrative audit, or audit of the operation of a specific internal organisation).[5] It is clear that audits not only facilitate economic investigations, but have rights that encompass the entire organisation. Data protection. In our age, the state of IT technology has enabled the creation and maintenance of an information society – at the same time, these very technologies make this society vulnerable. Accordingly, there is no question that its protection now requires modern systems arranged according to a strategy, which can keep up with technological development. In summary, we can say that while auditing and economic protection constitute a continuous and efficient control system and organisation, data protection, asset protection, and security technology assist the work of these control organisations, also providing control and service. Many models exist in the area of security technology specifically for the analysis and assessment of risks at hazardous plants, which are not part of my current work, but their applicability is also indispensable for the protection of private property. Security, data protection, and legal support assist the work of the entire security organisation and assume certain risks. In the following, I will examine the role of asset protection from the viewpoint of the investigation of damage events and disciplinary cases, for which it is important to clarify certain definitions.

Definitions

Let us examine a few definitions regarding what we consider damage. "Damage: event that causes a detriment or deterioration in the physical being or health of humans. Quantitative and qualitative reduction of assets". This shows us the definition of damage, but let us also see other examples of definitions from professional literature. [6p 276]

"Damage: damage refers to economic loss caused to the property of another through some reason. Damage is social if it was caused to property of the society. Damage may be caused by any conduct, act, or negligence as a result of which an asset is destroyed, eradicated, damaged, becomes unusable, is lost, a manufactured product becomes scrap etc. In such cases, if the damage is caused to an existing asset, we talk about actual damage."[7 p 212]

"Damage event: the combined circumstances and conditions, which as a consequence of a certain event result in the alteration, loss, depreciation, health impairment, or accident of another object or person."[8p 278]

"during the performance of personal- and asset protection or private investigation activities – as during any other activity - damage may be caused though various reasons to various persons or organisations. The interest of the victim is to be compensated for the damage they have sustained. The fundamental method of compensation is the compensation paid by the

party that caused the damage. In certain cases this involves compensation, and in one part of certain cases insurance that covers all or part of the damage."[9p 81]

It is evident that various examples in professional literature specify the definition of damage and its origin quite precisely. Whoever causes damage to another shall have to compensate that.[10] Any given organisation or company must define its own interpretations and concepts, as the significance of a certain type of damage may depend on the activity and nature of the manufacturer. For some organisations, the loss or destruction of intellectual property and their research and development activity may require far greater security and attention then their tangible assets. Examples include software development companies, as well as financial enterprises and research and development laboratories. Assets (may) include not only the object, but also the intellectual activity itself; therefore it is very important that the given organisation has to map and define right from the outset what they refer to as property or assets and what they shall include in their range, as without this it is difficult to set up the investigative organisation correctly. Despite differences in their regulations and character, the creation of three asset groups is recommended for manufacturing plants.

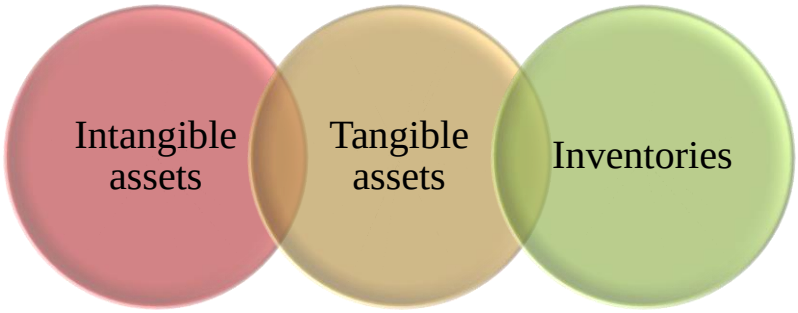

Figure 2 Asset groups (author: L. Kálmán)

Assets may be intangible, tangible, or inventories. Intangible assets consist of intellectual property, while tangible assets refer to the totality of assets indispensable for work. Inventories are the finished products manufactured by the plant, also including raw materials, excipients, and active ingredients required for production. It is advisable to specify the procedural code followed by the company for cases of damage to assets. Damage may occur in a great number of ways (through personal responsibility, negligence, intentional acts, technical malfunction, accident, etc.) Due to technical reasons, scraps may also occur in connection with finished products – although this is a very serious production error – and the obsolescence of assets will also result in scraps; therefore it is advisable to operate the entire investigation process of damage events at companies through a unified system of disposal regulations. Rules must be defined for their regulatory process, regarding the treatment of a given asset at certain times, as well as the handling and obsolescence of intangible assets and the generation and registration of tangible assets, right up to their disposal or utilisation. This procedural system may also be used for finished products. The investigative organisation and its structure, which ensure suitable protection of our assets are also part of this procedural system.

Within the investigative system we must define which basic concepts the procedural code should deal with, as well as the basic procedural concepts we may encounter and how obsolescence of assets and inventories should be addressed. Qualification, expert opinion, and the re-utilisation of scraps are all important concepts, since the re-utilisation of certain assets

may compensate in part for their loss. The correct definition of the system of concepts used in the regulation is crucial.

Figure 3 The connection between definitions and controls (author: L. Kálmán)

Controls

Let us examine what controls should be used to ensure awareness of the managers exercising the rights of the employer and employees of their responsibilities, so that these controls allow even clearer interpretation of the law in order to avoid or limit damage. It is not only advisable, but also essential to define responsibilities clearly. One of the most evident and direct controls is a well-written job description. Job descriptions may contain different provisions about work and causing damage according to the organisational unit or type of work. The responsibilities of the persons in charge of warehouse stocks, those generating these stocks in the manufacturing plants, or of the persons exercising the rights of the employer are entirely different. Obvious differences need to be regulated in the job description, and should also be specified at an even higher level, in employment contracts. If possible, a code of conduct and a collective agreement should be drawn up and implemented, targeting the themes of conduct themselves – naturally, this typically applies to medium-sized or large companies and industrial facilities. The collective agreement must clearly lay down the responsibilities of both employer and employee. Employers also have a compensation obligation towards their employees. It is necessary define clearly for which issues, how, and to what extent compensation obligation is offered.

Employees must compensate damage caused through a breach of their obligations arising from their employment, provided that they did not act as could generally be expected of them in the given situation. Employers must compensate the damage suffered by employees in connection with their employment.[11] In accordance with these principles, already the collective agreement must clearly indicate in which organisations, in which cases, and how damage is to be compensated by both employee and employer. It is important that damage may be caused wholly independently of personal responsibility, due to technical malfunction, through negligence, or intentionally. The extent of the damage also greatly affects its gravity. We already mentioned when defining damage that damage can be caused not only to assets, but also to human life. This is one of the gravest forms of damage, which requires maximum attention when setting up protective security organisations.

The primary objective, task, and duty of the employer is to create the conditions of healthy and safe work. This basic principle must be given top priority and followed up on throughout the procedure. Regarding the rationale and importance of the organisation let us examine two concepts. The first of these is near miss: work accidents also include near misses, which are events related to the activity of the company, during which the persons in danger are inside the danger zone, but no personal injury is sustained, due to either luck or organisational or technical measures. Basically, accidents which could under the circumstances have led to personal injury and damage, but in which personal injury was not sustained, can be regarded as near misses. It is a clearly defined tenet of the investigation of work accidents, as well, that

in addition to mandatory investigative methods an independent investigation is also necessary, if possible. Why is this important?

The concept of damage has also been defined, but without independence and expertise, that is, external investigation, near misses cannot be investigated professionally; they require the involvement of the security technology organisation. What happens if the security organisation is provided by an external monitoring firm, while the internal system of investigation by the company itself? In such cases the investigation of a damage event or a disciplinary case within an organisation is conducted by the manager exercising the rights of the employer. A sensitive issue arises here: will they conduct their investigation truly independently? If a breach of technological discipline or rules or the implementation of incorrect technological processes "occurs" through their own fault, will they find themselves accountable and at fault? No. The chances of this are very slight. For this reason, too, it is very important that not only larger industrial facilities and companies, but also smaller ones should commission an independent, external expert investigative organisation, since the consequences and conclusions will allow them to avoid damage or minimise its risk in the future, which is the most important consideration. Accordingly, responsibilities, the definitions of damage and related concepts, and the extent of compensation must be specified through several processes and presented in an orderly fashion and simply in documents which are clear to both employer and employee.

Remembering this, we can define the concept of the security of administrative responsibility. This is actually not just a concept; I would instead call it administrative security, which guarantees that duties, rights and responsibilities are clear with regard to both work processes and technology. These responsibilities should be regulated – in the employment contract, collective agreement, code of conduct, controls, disposal regulations, and the warehouse liability agreement and its process.

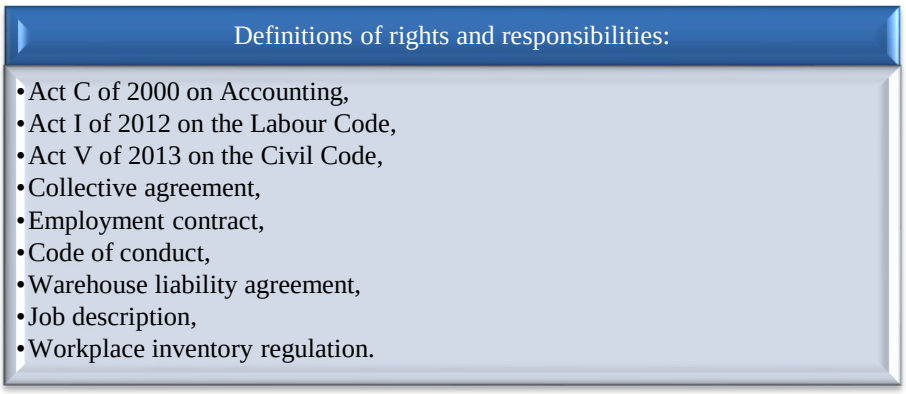

Figure 4 Administrative security (author: L. Kálmán)

It is very important that these regulations should be clear, binding for everyone, and accessible. Following the creation of regulations let us examine how the organisation providing the protection strategy can participate in operations. In order to protect assets, a Company Disposal Committee (CDC) needs to be set up. The name used for the Company Disposal Committee may of course be different at a given organisation – in the present case I will use this name. The members of this committee are permanent. As its head, it is advisable to select a senior manager: in manufacturing plants the production and logistics manager or their deputy or the top manager in the area production and logistics. Regarding tangible assets, members of the organisation usually include the manager in charge of procurement and maintenance contracts; for inventories, the material planning managers; for the generation of waste – which in some cases may also be hazardous waste – the security technology, fire

safety, and environmental safety managers, while designated members may include the experts and independent managers defined or appointed by the production and logistics managers.

Figure 5 Structure of the investigative organisation (Author: L. Kálmán)

The persons involved in control are the enforcement service that plays a part in asset protection or the head of the own-employed service, and investigating persons under their control. Independent members of the committee include the manager in charge of inventory activities at the company, that is, the manager in charge of inventories for the inventory group or class. On the basis of the information collected the committee decides on responsibility for the damage, gives proposals for further measures, and provides for the utilisation or disposal of assets that have become scrap. The rules for the utilisation, depreciation, accounting, and disposal of tangible assets also apply to all three asset groups listed previously (intangible assets, tangible assets, inventories). The detection of intangible assets which have become unnecessary, proposing their disposal, and conducting the disposal procedure are in every case the responsibility of the heads of the given functional areas, e.g. product development manager, IT manager. It can be seen clearly that already here the topmost managers are named as the persons in charge. The accounting of extraordinary depreciation is carried out based on the permission of the Chief Financial Officer of the organisation. The committee decides on the procedure to be used according to the submitted expert opinions and recommendations. The outcome of the procedure may be sale or destruction. Software products are destroyed on site, of which a protocol must be drawn up.

As a consequence, it is an important step to specify the heads and persons in charge of disposal and intangible assets and to define the disposal method as precisely as possible. Although the destruction of software can usually only be carried out on site, its method and tools need to be defined: which data carriers require breakage, deletion, permanent deletion, cutting, or shredding, as defined by the procedure and the quality of the intellectual product. Disposal may only take place with the approval of the Chief Financial Officer, based on expert opinions and the recommendations of professional areas. Let us now examine the return of tangible assets. Unnecessary assets must always be returned by the person to whom

they were entrusted to the person in charge of the given organisational unit, with documentation and justification.

Traceability is very important for the specified forms and is an indispensable condition for the investigative system and organisation, as well. Intangible and tangible assets and inventories alike may only be handed over or transferred with strict documentary discipline, as only this way can the investigative organisation determine subsequently how and through which channel given products were resold or possibly disposed of. Ensuring the traceability of the process is a very important security issue. The registration, collection, and evaluation of forms, transport documents, and delivery notes subject to strict tracking requirements are crucial in the life of a large industrial company, given the extent of their movement and flow of materials. Naturally, this also depends on physical location, but one thing is certain: the movement, flow, and logistics of both service equipment and finished or other products at a manufacturing plant are highly complex and interrelated tasks, which must be tracked precisely through up-to-date IT support; therefore IT support must be implemented through some form of business management systems. This traceability will be vital for subsequent investigations.

Objective of the regulation

For the regulation and the organisation to be created, their objective must be defined: controlling accounting and registers, strengthening documentary discipline, ensuring the veracity of the balance sheet through the correct determination of assets and resources, protecting company assets, ensuring the accountability of the persons financially responsible, and detecting depreciated inventories and out-of-use assets.

The method used to investigate damage events must be described in a clearly regulated fashion – any destruction, material loss, becoming unfit for use, or equipment malfunction of company assets due to natural disaster, criminal act, wilful act, negligence, or incorrect use of technology is considered a damage event. Following a damage event, the head of the competent organisational unit shall immediately notify the chairman of the regional disposal committee, and within 24 hours shall draw up the written protocol on the damage event, notifying the head of the asset protection investigative organisation with its transmission. What must the damage event protocol contain? In every case, the structure of the damage event protocol must allow the organisation conducting the investigation to discover as many details and events as possible. Naturally, this is only part of the investigation, which does not consist of the protocol alone. It is recommended that the protocol contain the designation and exact location and time of the event, the description of the damage, any preliminary events together with additional circumstances, the extent of the damage, and the cause of its occurrence.

The cause of damage may be intentional act, negligence, accident, natural disaster, or technical malfunction. The protocol must also contain the name of the person(s) presumed to have caused the damage, evidence relating to the event, the list of persons present, further comments and measures connected with the case, the statement on compensation, and the date and signature. Following the receipt of the protocol, further investigation is conducted by the private asset protection service or the protection organisation, which shall submit the result of the investigation to the independent member of the asset disposal committee - the head of the inventory group. The head of the inventory group shall submit the damage event protocol to the company disposal committee, who determine the person(s) responsible on the basis of the facts. Following this, assets may be delisted, resold, disposed of, or in some cases submitted for further controls or other procedural stages (official, insurance, civil law stage). Here, we must also define what happens if the perpetrator of the damage is not an employee of the company.

The procedure applied in the case of material damage caused by an outside worker, an employee of an external company, person, or organisation in a contractual relation with the company is identical to that described above, complemented by the fact that the company shall claim compensation for the damage caused from the perpetrator of the damage in a civil case. If the perpetrator of damage does not acknowledge or compensate the damage, the company may take measures to enforce its rights. It may initiate a criminal or civil procedure, whose beneficiary, according to the general principles, is in every case the top management of the given company. In the case of insurance events, the investigation protocol on the damage must be sent without fail to the manager representing the insurance organisation, who shall take further measures.

All damages must be entered in the accounts: for tangible assets, this is carried out by the registration group, while for inventories by the competent warehouses. If a defect is found upon receipt of a shipment of materials, inventories, goods, excipients, or active substances purchased by the company, measures must be taken against the supplier, to be implemented between the person who signed the contract and the company, with a claim presented against the contractual partner. In accordance with the rules of administrative security, the disposal committee encompasses several organisations within the company, as well.

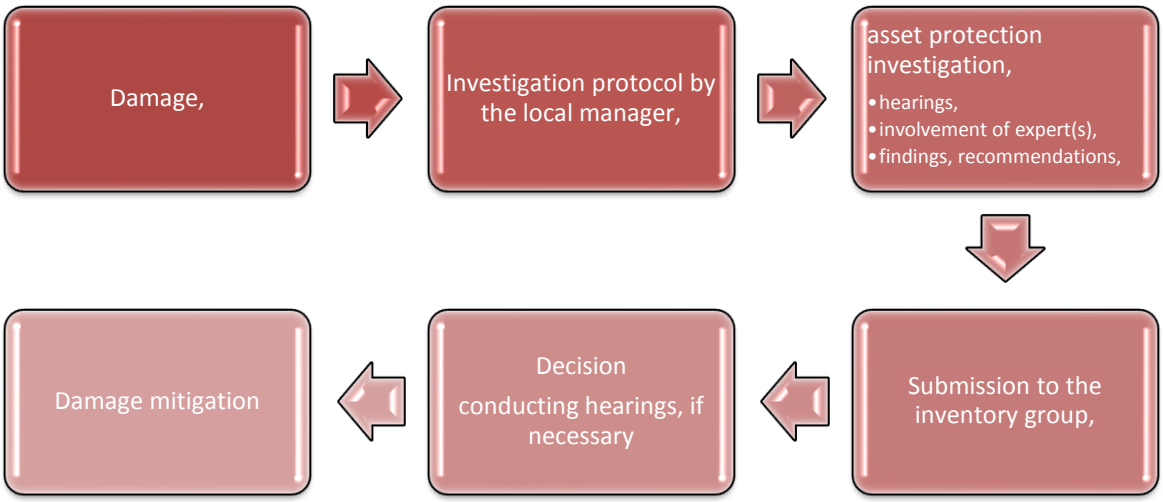

Figure 6 Investigation process (author: L. Kálmán)

It is very important that the own-staffed asset protection service of the security organisation conduct an investigation, as it is based on their recommendations and findings that personal responsibility can be determined, but it is even more important that during every investigation it is advisable and vital to draw conclusions that will clearly allow similar damage to be avoided or prevented in the future. The recommendations resulting from the investigation must contain conclusions through which the occurrence of similar cases can be avoided in the future.

What methods does the security organisation use? Their primary method is the collection and analysis of data. They cannot act as experts in every area, nor is this necessary; however, they must involve experts, drawing and compiling the correct conclusions with their assistance.

In the first step, the question of powers and competence should be examined in every case. Depending on the magnitude, extent, and nature of the damage the case may require internal investigation or, in the case of accidents, possible intervention by the authorities, that is, an investigation by the police, fire safety-, disaster management-, work safety- or other authorities. In such cases, the local security organisation does not conduct its own investigation (which would not be practical); instead it must rely on the findings and results of the official investigations, but must provide data, site securement, and fact-finding, as requested by official bodies and transmit the available information to them without fail, in every case supporting the investigation. If the investigation is conducted internally, they must determine personal responsibility on the basis of the damage event protocol, together with the compilation of photographs, videos, and evidence and site securement. Following the determination of personal responsibility they will make recommendations, taking all circumstances fully into account, in order to determine whether the event was caused intentionally, through negligence, or by accident.

The investigation of the security organisation in itself will not result in disciplinary action against own personnel. The conduct of disciplinary proceedings is the right and responsibility of the manager exercising the rights of the employer. The security service acts as a support service, which investigates the case, finds evidence, draws up a summary report on the case, conducts hearings, and presents these results to the competent manager exercising the rights of the employer, the previously mentioned inventory organisation, and the committee set up for further handling of the asset. We can say that it has rights to express its opinion and summarise the case. As I mentioned earlier, it is very important that the summary report of every protocol should contain conclusions as to how the damage events which occurred could be avoided and what safety measures could be introduced within the organisation itself and in production and technological processes, which would help prevent a future reoccurrence of the damage event. Without such conclusions the investigation is of limited value. Naturally, changes to individual technological processes on account of the conclusions are not the task of the security organisation. Appointed engineers and experts are available for this – moreover, the fact and conclusion that a problem is identified in a technological process, which caused the malfunction, must generate further review by the manager in charge of the given process. If this does not take place, and the same damage event occurs in the future due to their not having reviewed the process, the manager in charge of technological processes, too, can be held responsible. For this reason, due care is extremely important.

Protocol

In the investigation of the case, the protocol of the hearing must be signed by both the person concerned and the witnesses. As the basic principle of the protocol of the hearing, let us take the quote on the administrative hearing from the Manual of Security Technology by Vendel Kovács: “Hearing of the information known to the person related to the acts being investigated, during a personal meeting. It may take place in the presence of witnesses, whose names must be recorded, with a protocol drawn up. The enforcement body may only conduct disciplinary proceedings with regard to its own employees and only if this is in line with the nature of the given proceedings; nonetheless, the head of the financial organisation may give them mandate to conduct other disciplinary proceedings, as well. The purpose of the hearing and internal regulations must be indicated in the protocol, and effort should be made to make literal and pertinent records. A protocol must be drawn up of every administrative or asset protection hearing, damage event, or report, in a sufficient number of copies so that the person making a declaration may receive one of those. The potential conflict of interest of the person recording the protocol must be examined; that is, they may not be related to the person who is the subject of the protocol.[12 p 67]

The administrative protocol should, therefore, be drawn up according to the basic principles and the following: It must include the location and exact time the protocol on the hearing is drawn up, the name, identification, and details of the person being heard, the persons present, the person in charge of and the person recording the protocol, and witnesses. It is advisable that the manager exercising the rights of the employer be present already when the protocol on the hearing is being drawn up. This is important as this way they can immediately obtain information and can ask any of their own questions in order to clarify the matter, and also because they are more knowledgeable about processes. A vital issue in connection with the protocol on the hearing is that a hearing is not an interrogation. Interrogation falls within the competence of the authorities. The protocol on the hearing must limit itself to the essential elements, the person being heard must be informed of the method of its recording, and their words must be recorded either literally or as abridged quotes, with their participation, but mandatorily with their consent. It is advisable, and based on my professional experience the best solution to record questions and answers literally. Every protocol must concluded with a question to the person being heard as to whether they have any objections to the way the protocol was recorded and whether they wish to lodge a complaint, with regard to which a clear declaration must be obtained from them. The person being heard has the right to read the protocol even several times, and amend literal quotes of their answers, following which they must sign it in approval.

Summary of the event

The summary report is compiled from the protocol drawn up, witness hearings, and requested expert opinions. The summary report already contains essential findings and facts, with expert opinions, protocols, and the information and facts collected by the asset protection security organisation (images, information, objects, etc.) as its attachments. Following the presentation of the summary report the decision is made on both action against the person(s) responsible and further handling of the damage, be it reutilisation, processing, disposal, sale, or destruction. Protocols not only play a role in the investigation, but are also required by law as proof of e.g. accounting or the destruction or depreciation of tangible assets before authorities. Organisations which exercise due care can achieve considerable financial savings through conducting damage event or disciplinary proceedings. How do we achieve this? Thorough investigations promote more organised and disciplined work. In some cases, the findings of an investigation can bring about developments that can minimise the risk of damage events, so the results of the investigation can be monitored clearly

Analysis

What else can be done? In our modern world, IT tools can be involved. Through the development of IT tools, we can create a risk analysis system in which, by recording cases, we can define, monitor, and statistically examine various events within a given industrial organisational unit. It matters, and is in fact of almost inestimable significance if we can know how many and what type of events occur most frequently in which unit of a given organisation. If instead of a decreasing tendency these show reoccurrences, feedback must be given to the given organisation. If the situation still does not improve, the highest-level organisation monitoring the given organisation must be notified. For example, if damage events, damage caused by employees, accidents, negligence, accidental crushing or dropping of packages keep occurring at a warehouse, the composition of its personnel, and in some cases the competence of its leaders must be examined. Statistics, monitoring, and risk analysis help improve the efficiency of companies. Determining the range of unlawful appropriation by employees and identifying the method and location of instances of such are an indispensable basis for elaborating the correct protection strategy.

Manufacturing plants consist of a production area and various logistics areas. It is essential to define clearly from which processes and points of production and logistics unlawful appropriation by employees, that is, theft, may occur. On the basis of this information the security organisation can act in targeted manner, possibly in cooperation with the authorities, to investigate unlawful appropriation and perpetrators acting intentionally and in some cases in an organised form. Risk analyses, therefore, are of great help in protecting company property. The IT infrastructure of these risk analyses is vital, especially if our company is large. This is because the larger a company, the greater the numbers of its sites, staff, equipment, excipients and active substances used to manufacture a given product, and the more diverse its finished products, the more complex this system will be, which cannot be tracked clearly without administrative monitoring, making risk analysis indispensable. I can say that today one of the fundamental pillars of prevention is proper and efficient security, which requires correct risk analysis. From the number of internal risks and hazard sources and the factors related to their existence both managers working in the area of asset protection and the management and proprietors of the company can draw a large number of conclusions.

There are several tried and tested models for security technology, especially with regard to larger chemical plants (Dominó XL, the Dutch filtering method, HAZOP operability and risk analysis, Fault tree analysis, Preliminary risk analysis, etc.).

"Risk analysis is the methodical use of available information in order to identify risks. Risk analysis is composed of the definition of the scope of the analysis, the identification of related risks, and estimating these risks. Risk assessment can be divided into the partial processes of risk analysis and risk evaluation. Hazard identification is the process of recognising the existence of hazards and defining their characteristics. Risk estimation is the process used to determine the extent of the analysed risks. Risk estimation consists of the following steps: analysis of frequency, analysis of consequences, and their integration. The second step of risk assessment is risk evaluation, a process in which the acceptability of the risk is evaluated on the basis of the risk analysis. Risk control refers to the decision-making process related to the management and/or reduction of risks."[13]

It is advisable to present the ongoing report regularly and periodically to top management. The figures, factors, and indicators that can be defined in this report are unambiguous. If we refer to them as summary or collective reports, then police, disciplinary, and damage event cases should be handled and analysed in a consolidated fashion at the level of the company and their information must be shared with management. Internal asset protection risk analysis software products are still rare on the market, but they can definitely be developed. Several programs are suitable for this; in fact, just with knowledge of Excel they can be learnt and created, and later connected to databases and programs. If we can define this clearly, we will soon find the perpetrator of unlawful appropriation. In summary, we can say that internal security and protection within an organisational unit can only be ensured in a targeted fashion, through cooperation with several organisational units and all security technology personnel, and in harmony and fusion with managers and employees alike.

The staff numbers of the protection organisation must be optimised and stability should be a goal, since – just as is many other areas of life – the more stable good staff is, with low fluctuation, the more efficient the security personnel will be. For this reason, the question of whether to use own manpower or an external, contracted company for custody and protection is an interesting and sensitive one. The organisation can also function well with an external company – custody using own manpower was just an example - but in this case different methods must be used. The external organisation must be required to carry out its tasks in a stable and efficient manner and an own organisation must be set up in parallel, which carries out internal investigation activities. The only difficulty – and a sensitive issue – can be that the flow and collection of information and data provision may become cumbersome in this

organisation structure, but this does not mean that it cannot fulfil its task. This works differently across industrial units, since every organisation must create its protection strategy differently, but the basics are the same. The theoretical conclusion that the protection organisation and strategy must be created in a regulated manner is more and more evident in the needs of every organisation.

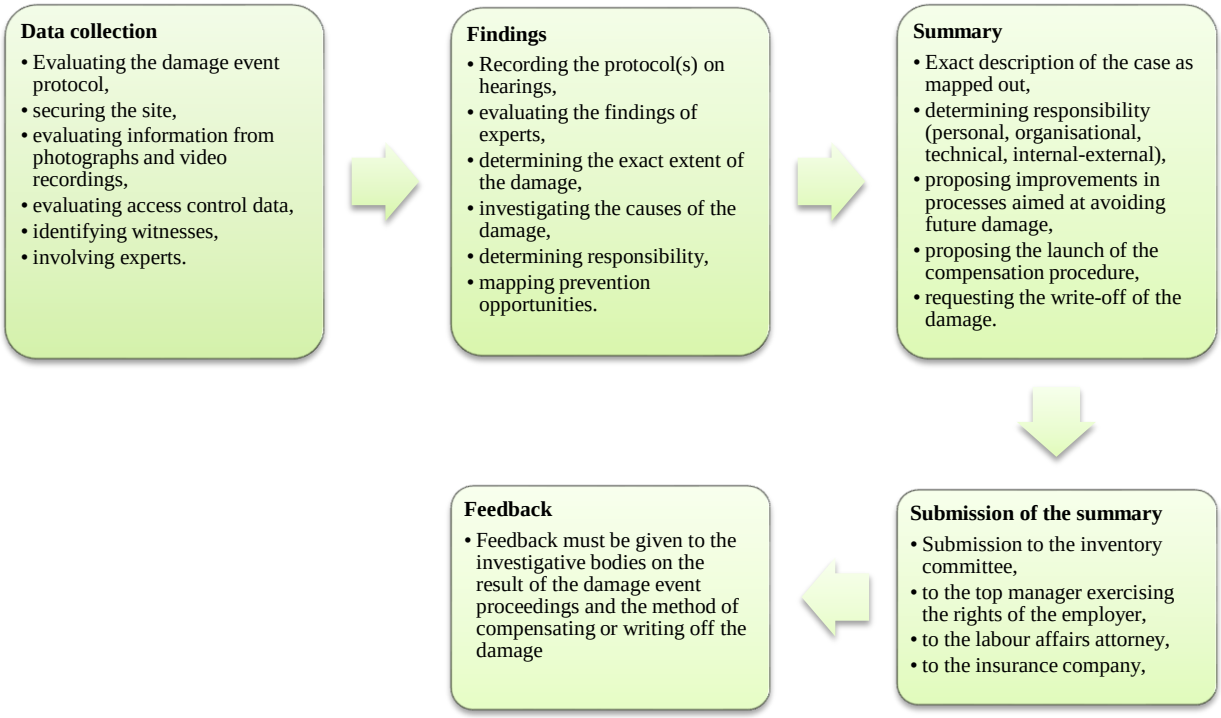

Figure 7 Security investigation processes (Author: L. Kálmán)

Conclusion

During internal investigations an efficient protection organisation must be forward-looking and must think, assess, evaluate, and analyse risks carefully in every case. The fact that an independent security investigation is an indispensable part of investigative methods within an organisation, with inestimable efficiency is also clearly borne out by the above. We can conclude that a correctly organised protective structure generates not only savings, but also further opportunities. Thanks to it analytical programs can be linked to risk analysis and production, and certain indicators can be added, thus enabling their even greater efficiency.

The security organisation can not only analyse cases efficiently, but can also prepare for unexpected situations, thus knowing beforehand when and in which phase a given area must be strengthened in terms of security technology or asset protection, or which technological processes a manager needs to pay more attention to. This requires further developments, but risk analysis and the use of these software products enable an outlook that can lead to a highly efficient organisation which can generate above-average profits, since if our assets are not lost and our damages are lower, we will possess more useable assets and materials. The value of this is inestimable. It would be hard to put a figure on it for comparisons, but its result is tangible and could be used as the basis for further studies. In the life of an organisation indicators can show the efficiency of detection and of the security service in their investigative tasks for both disciplinary cases and damage events. With regard to the future, we need to consider the development of the electronic equipment, software, and applications of asset protection, as we need to monitor the development of not only protective alarm and camera systems, but also the elaboration of our protection system and strategy. We can say

that risk analyses and the IT support they require do not address our concerns suitably at present. I believe that this is where the future and savings lie. We need to protect ourselves not only against outside intrusion, but also other forms of damage. Prevention is more important than damage limitation. We can achieve considerable savings with intelligent, analytical IT support with an evaluating outlook. At the same time, we need to monitor the analytical integration of protection systems, which together with analyses open up new avenues for improving the protection of private property.

BIBLIOGRAPHY

[1] L. BEREK, T. BEREK, L. BEREK: *Személy és Vagyonbiztonság (Personal and Asset Security*), Budapest: Óbuda University, 2016.

[2] BEREK L.: *Biztonságtechnika* (Security Technology), Budapest: National University of Public Service,

[3] AMON G.: *A korrupció jelei a beszerzési folyamatokban (Signs of corruption in procurement processes)* https://view.officeapps.live.com/op/view.aspx?src=http%3A%2F%2Fwww.mkvk.hu%2Fletolthetoanyagok%2Fkonferencia%2Fokk%2F2010%2Feloadasok%2FAmonGabor.doc downloaded: 30-04-2017

[4] VEIT K.: *Szakmai szkepticizmus a könyvvizsgálatban A csalásfelderítés és szakmai szkepticizmus közötti kapcsolat (Professional scepticism in auditing – the relation between fraud detection and professional scepticism)* http://new.szak-ma.hu/data/cikk/10/81/cikk_100081/VeitKrisztina-Szakmai szkepticizmus_a konyvvizsgalatban.pdf downloaded: 30-04-2017

[5] *Course material: Audit types* http://www.szervez.uni-miskolc.hu/blaci/minmen/audittpusok.html downloaded: 30-04-2017

[6][8] TAKÁCS Gy.: *Vagyonvédelmi Fogalomtár (Glossary of Asset Protection),*1986 publisher: Machine Industry Scientific Association ISBN 963 444 000 2

[7] SZITTYAI A.: *Üzemrendészeti Kézikönyv (Manual of Plant Security)* VI. 1974

[9] KÁLÓ J.: *4. fejezet, szerkesztő: György SZÖVÉNYI Biztonságvédelmi Kézikönyv (Manual of Security Protection)* 2000 ISBN 963 224 553 9

[10] *Act V of 2013 on the Civil Code, Chapter XXVI Section 6*:519, 30-04-2017

[11] *Act I of 2012 on the Labour Code, Chapter XIII Section 72 Responsibility for damage caused*, 30-04-2017

[12] KOVÁCS V.*: Biztonsági Kézikönyv (Security Manual)* 1997 ISBN 963 04 7865x

[13] ABONYI J., FÜLEP T.: *Biztonságkritikus rendszerek Kockázatelemzés és kockázatmenedzsment (Safety-critical systems. Risk analysis and risk management)* http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch02.html downloaded: 30-04-2017