



{ The system's operation must
be efficient, but also intuitive
and as simple as possible }

4. Intrusion Detection “The Smart Way”

Arjan Bouter & Rene Waenink

Intrusion detection

Every company invests in measures to prevent intrusion. Conditions and guidelines for intrusion detection systems are usually laid down by insurers. Even when this is not the case, insurers' guidelines are often observed. Because the related investments are considerable, we often assume that intrusion prevention is well organised within our organisations. But is this really the case?

A conversation with security managers from a few different organisations quickly shows that, in practice, things are often different. The installation and use of an intrusion detection system often causes more trouble than it is worth and it does not produce any measurable benefit for the company. This article will discuss a few technological developments that can be employed for the improvement of the manageability and operation of intrusion detection systems. We will also discuss how we can ensure sufficient information and proper reaction if something actually occurs.

Let us compare the news after an intrusion incident with the spreading of news around the world. Important news, including images, sound and commentary (interpretation of the information), spreads in just a matter of minutes around the world. Through consulting several sources we can provide ourselves with an objective and complete picture of what has actually happened.

An intrusion incident is important news for those in charge of a company. Objective sources, such as intrusion detection systems, fire detection systems, access control systems, intercom and video systems can provide us with information about the incident. Intrusion and fire detection systems usually provide information to a control room (PAC). All other information is usually investigated after the incident has occurred. Simultaneous presentation of information from multiple sources only appears to be available to a very small number of organisations who have invested heavily in an umbrella security management system.

Although insurers usually reimburse the costs after an intrusion incident, we should definitely ask ourselves what we are actually achieving with our current intrusion detection systems. Asking several accountable security managers this question quickly resulted in the following statements:

- “I have had so many false alarms that the alertness of follow-up services has dropped to a minimum.”
- “I could put the extra expenditure for following up false alarms to better use.”
- “In spite of all the investments, goods have gone missing because the intrusion detection system was switched off at the time.”
- “I am growing with my organisation, but the intrusion detection system cannot.”
- “I do not have any direct knowledge regarding by whom, when and where the intrusion detection system is operated.”
- “I do not have a good overview in the case of an alarm. The combination of data from the intrusion detection system with other security systems such as cameras and access control would be helpful, but is too much bother.”
- “The operation of the intrusion detection system is fairly complicated. My employees regularly make mistakes so that I still have to return to the property myself.”

Market developments

What have suppliers of intrusion detection systems and the legislators done about the problems just discussed in the last few years? Here is a brief overview:

Legislation

Following the first legislation in the eighties (“REB’83” in the Netherlands), a new form of legislation was adopted (“BORG” in the Netherlands). Part of the objective was to reduce the number of false alarms. An attempt was made to give quality a considerable push by introducing certification for the products and the people who install these systems. The result: almost as many false alarms as before. The cause was the human factor. A factor that is difficult to influence. People sometimes make mistakes that they are aware of, but more often they make mistakes they are unaware of. This is why the latest trend is to verify alarms before sending emergency services to the location. The root of this idea is of course good, but people seem to have accepted that further reduction of user errors is no longer possible.

Technology

In comparison to other industries, such as the CCTV systems industry, not much attention has been paid to technology in the intrusion detection industry. Detectors have been improved and protected from interference, but the central equipment has hardly been developed at all. Intrusion detection systems are still limited by a number of zones and areas. A few suppliers have introduced a card or key fob as a medium for arming or disarming the system. In the area of communicating incidents developments are slow, with increasingly detailed information being received by the communications room. Unfortunately, all the attention appears to be focused on the medium conveying the information (such as analogue, ISDN and IP). The emphasis is often not on the completeness of the information, which would really facilitate better decisions being made regarding the handling of alarms and incidents.

Integration

The latest legislative trend concerns the integration of intrusion detection with sound and images. Through the combination of different systems (or linking them together), far more opportunities for the prevention of false alarms through verification are provided. Consequently better controls before alarm activation are available. In the past, combinations were made through linking systems together. This often was realised through contacts at hardware level. The next step was the deployment of umbrella software for the integration of the systems. These security management systems were often exclusively used by larger companies due to the level of investment required. Truly centralised integrated security systems,

in which information from systems for fire, intrusion and access control with video and sound is linked together and combined into one incident-related package for control rooms, are certainly not widely available.

Ease of operation

The operation of intrusion systems has migrated from keys to PIN codes. In recent years, these PIN codes were replaced with a card or key fob or a combination of both. The operation itself however has remained unchanged. Complicated menu structures to engage the correct section or to inhibit a zone remain. And displaying, for example, an unlocked door on the alarm panel also remains very complicated, which raises the chance of human errors occurring considerably.

We can conclude that legislation is primarily aimed at producing more information for the verification of an alarm notification and that the developments in this area are not very progressive. If we compare this to other areas within the security market, it is fair say that innovative development is slow. The most significant reason for this is that legislation hampers the introduction and deployment of new products.

New developments

Which ingredients are necessary to motivate the intrusion detection industry to find answers to the current challenges in the market?

First of all, it needs to be more widely accepted that a good system need not follow existing rules and legislation. **By definition, legislation is out of date and often hinders the deployment of new developments.** It would be better if legislation was more often based on intrinsic objectives, such as the generation of a maximum of one false alarm in each period. Through setting targets rather than drawing up rules, supply and demand find each other more quickly and the requirements set by the government are safeguarded.

Technical developments within the intrusion detection system industry are focused on the medium for transporting the alarm. Less attention goes to improving the quality of alarm-related information. Manufacturers are cautiously beginning to use web-based applications for consumers. This gives the owner a clearer picture of events and alarm management in his system. Unfortunately, this kind of service is not yet available to companies

that have to cover numerous risks every day. Even so, there are some recent developments in the market that could provide a solution to everyday intrusion problems. These developments are at an architectural level. New, cleverly designed architectures can help to bypass the current technical limitations.

New architecture

What does the architecture required for an effective intrusion detection system look like? What requirements do we apply to the architecture of future intrusion detection and security systems? A first requirement concerns the scalability of the system: this must no longer be an issue. Whether there is one detector or a thousand, whether there is one section or as many as a thousand, the system should not limit the customer in its ambition to implement an effective and efficient intrusion detection and prevention system. The result of increased scalability is that more and smaller sections are easier for fewer people to manage, thus reducing the number of arming and disarming errors.

The linking of intrusion detection centres and/or detectors to IP networks must be easily possible. Convergence into a single network infrastructure delivers tremendous cost savings. Local equipment must of course be able to operate independently of the IP network. This makes it no longer necessary to generate alarms for the communications room from a single point: alarms can be generated from multiple independently operating positions. After all, security is about managing risks.

The security controller will have to be configured with multiple functionalities. This means that, in addition to, for example, intrusion and fire detection, there must be a facility for the storage of access control, speech and image data. Because the needs for this may be different for each situation, this means that settings can be made during installation and changed or expanded at any given moment afterwards. There is not just convergence at network level, but also at hardware level. Incorporating multiple functions into one single hardware platform simplifies the linking of objective information from several sources and the transmission of this information to the systems and organisations established for this.

The next requirement is the effective presentation of information and the easy operation of the system. Information has to be displayed in a way that is clear, unequivocal and simple to interpret.

The system’s operation must be efficient, but also intuitive and as easy as possible. This is easy to say, but in practice it is much more difficult. It is important that the architecture is such that it serves the users as good as possible. A good presentation also shows who last armed the system. This information must be displayed clearly, stating name, photo, date/time and a recorded image to support the intrusion management process.

It also is an important requirement that accurate data is employed in the system and that data is displayed completely and only to the right person. This means that, for example, the personal data registered in a central database must be linked to the HR system. This ensures that employees who leave the organisation are automatically erased from the security systems and can no longer make use of cards, PIN codes, etc.

New architectures offer many possibilities and are often already applied where legislation has no influence, within multinationals for example.

Practical use of intrusion detection systems

It has already been stated that some necessary changes have already been made to the architecture of intrusion detection systems and that further necessary changes will follow in the near future. Presenting adequate and relevant information about intrusion, fire detection, access control, video and speech to the people responsible is easier to achieve these days. It is consequently worthwhile to re-examine the manner in which the intrusion detection system is operated. Most errors are made by people when arming and disarming the system.

Arming and disarming of the intrusion detection system by users

Let us have a closer look at what can happen during the arming of an alarm system. Questions that could arise are: What is the code? Have I switched the lights off? Am I really the last one in the building? Are all the windows and doors closed? I see a message in the display, but what does it mean? Errors made during the arming of the system often cause false alarms.

The following recommendations apply to effectively arming and disarming intrusion detection systems, which consequently reduces the number of false alarms.

Preparation

In the security management system it will be determined for each department (office) which people are responsible for the intrusion detection system. Telephone numbers, email addresses and instructions are linked to this information. Each office can exist of multiple zones in multiple buildings. In each office, personnel is authorised to operate the alarm. Authorisations are only applied if the responsible security officer has given permissions and if adequate instruction has been provided. Only after the intrusion system operation instruction has occurred, is the user authorised to operate the system.

The objective is to send sufficient, relevant and the right information to the correct person in the case of an incident. Besides providing instruction to the users of the intrusion system, any person entering the building should have been instructed how to react when an alarm is generated.

What medium should be employed for arming and disarming?

Currently, it is possible to choose from a range of options for arming an intrusion detection system: from a PIN code, card, or biometric identification to a combination of various methods. Irrespective of the medium employed, this will still have to be managed in a security management system. An employee who leaves employment or is blocked should not be able to use this medium.

The disadvantage of using a PIN code is that it can be “forgotten” or an error can be made when entering it. Consequently, an access badge for operating the system is a better option. This prevents entry errors and appropriate sections or zones are automatically selected. A disadvantage of using an access badge is that if loss of the badge is not reported, there is an immediate risk. This is why most systems employ a combination of a code and an access badge. An even better option would actually be to arm or disarm the system using a badge and a form of biometric verification. These technologies are nowadays **sufficiently reliable** and are already **widely available**. The implementation would be to only allow intrusion system operation after biometric verification (i.e. fingerprint or iris scan) of the person's identity.

Authorisation levels

In addition to the assignment of appropriate zones to a person, the security management system must also be able to assign specific

authorisation levels. This authorisation level indicates the degree to which a person is authorised to operate the intrusion system.

Possible levels are:

- Level 1** Only arming of the assigned zones.
- Level 2** Arming and disarming of the assigned zones.
- Level 3** Free choice of arming and disarming zones, inhibiting zones and resetting of alarms.
- Level 4** As level 3 with addition of forced arming (arming with open zones).

The correct assignment of these levels simplifies the operation for the users. After all, the menu for level 1 has fewer options than level 3.

The arming process

After arming the display shows the following information:

- Open zones (doors and/or detectors). It is indicated if there are goods obstructing the detectors (anti-masking).
- people still present in those areas (applicable if presence/absence registration is in operation).
- authorised person available for assistance.

If there are no people present in the areas and the zones are closed, arming can take place. During the arming process and afterwards, all the access doors to these zones are automatically blocked. This prevents an error from occurring because of someone entering through another door during the arming process.

Using the data in the security management system it is possible to register which people are present in an area. It is therefore not necessary to perform a presence/absence registration for each zone providing that a proper presence/absence registration (with anti-pass back) is applied to the outer perimeter.

Once the arming process has taken place, any lights that are still burning can be switched off and the night lighting can be activated.

Open zones are shown on the display using a map. If the system cannot be armed, a message or instruction with relevant information can be sent to the authorised person (e.g. security officer) using the display. Also a speech connection can be activated for consultation, simply by pressing a button

The disarming process

If the intrusion system is armed, all access badges will be rejected by the card readers. Exceptions can be made in cases of fire and other emergencies and for specially authorised people. Authorised people who wish to disarm the system in a section can indicate this by offering their identifier medium (i.e. badge) to the operation terminals. The selected section(s) or zones will be disarmed automatically after the confirmation question: “Do you wish to disarm?” has been answered. Card readers that were blocked prior to operation are now reactivated again. If desired, the lights can be turned on automatically for the person now entering the office. This feature contributes to the “green building” certificate and corresponding grants.

Block times

It is usual in intrusion detection systems to agree on block times. These block times are usually monitored by the control room and they are triggered if the system has not been armed or is disarmed during these block times. Block times should be registered in the intrusion system so that parts of the arming and disarming process can be automated. Templates can be used to define who may arm/disarm, when, and where.

Checks on the system state are performed at predefined times and users may receive an email or text message about the system state that is automatically generated by the system itself. This procedure continues to run automatically, if desired for multiple people, until the system is disarmed. Of course, this task can also be performed by the control room.

Information, control and means of control

In addition to improving the arming and disarming process itself, there is also still a lot of room for improvement if it comes to the way intrusion related information is presented to system managers.

To be able to properly manage the arming and disarming process of the various sections and zones, it would make sense to record the arming and disarming moments with additional information such as date/time, operation place and stored video images for reviewing the operation itself and for verification of the identity of people. Multiple erroneous entries of, for example, the PIN code will be registered. After three attempts, further access is blocked and the responsible people will be informed automatically.

An alarm that is generated immediately after arming and disarming the system will be sent to the authorised person by email and/or text message. This includes information about the location, date/time, operator contact details and video images from the moment at which the operation took place. Immediate remote follow up is possible using this information. As an extra check, this alarm can also be dealt with separately by the control room.

When operators make errors during arming and disarming, they are added to a list. This way, at any moment an overview is available of people that may require extra instruction or assistance. To implement an improvement process following an operating error, an email can be sent to the person that made the mistake with additional arming instructions or with a request to contact the responsible security officer.

After causing an operational alarm multiple times within a specified period, the arming medium for this person is blocked. This person is requested to report for further instruction.

As previously mentioned, a requirement for a modern system is that operating errors are prevented as much as possible. A good user interface allows people to perform their tasks quickly, but also ensures that the chance of errors is small. A good interface also supports trial-and-error mechanisms to teach users how to operate the system. Good feedback on errors is essential here. Modern systems are also able to adjust the operation of the system and the display of information dynamically and sometimes even automatically adjust themselves realtime to the behaviour of the users.

Proper alarm follow-up

At the moment an alarm is received, two things are of importance.

- Reaching follow-up people to check the site as quickly as possible.
- Getting a complete overview of the situation.

Because systems and devices are able to exchange information, it is possible to not only collect the following information locally but also in the control room or even from a remote location:

- Information about the property: address, place, street, etc.
- Information about the alarm: type of alarm, property, floor, detector.
- Information about authorised people: responsibilities for this department/alarm follow-up.

- Images from (IP) cameras during the alarm.
- Images from (IP) cameras during the arming/disarming with name, telephone number and photo.
- Names and photos of people who have offered access badges to card readers (in the vicinity).

Because all this information is available from the database, further compilation of this information into one comprehensice incident related package during an alarm situation is easily achievable. The manner in which this information is made available can be adapted to suit the organisation:

1. Directly to a PAC for further alarm settlement.
2. By email and text message to the responsible people from the section. Possibly also with read/receipt confirmation.
3. As an addition, footage of the incident that generated the alarm can also be played back.

Finally

The guidelines discussed here to prevent false alarms and to provide improved information about intrusion related incidents seem obvious. Although legislation outlines the intrusion environment for organisations, it is clearly visible that companies these days very often choose to implement alternative, more effective scenarios. Experience has already proven us that this can lead to better manageable situations. Using the outstanding technology that is already available makes the investment in modernised intrusion detection and security systems even more feasible.

The trend for the coming years will be the proper compilation of security incidents related information (data, images, and speech) and the delivery of this information in a smart way to the responsible peope. [Concepts like the security controller may be of great value to realise these effective intrusion detection systems.](#)

In addition to proper alarm handling and incident management, modern systems also appear to be better at avoiding falsely generated alarms. The inputs from several different devices (PIR, magnetic contacts, camera, etc.) are cleverly combined. No single PIR or contact generates an alarm, only predefined combinations. It is most likely that the more sensitive detectors, armed automatically only after approval of the primary detectors, will indicate there is sufficient reason to generate an alarm.

Modern systems facilitate interesting applications. However, it seems important to always remember our primary objective: minimising intrusion related damage for our organisation through the most efficient and effective deployment of tools such as the intrusion detection system. With this focus in mind we will be able to successfully implement most interesting intrusion detection and security management scenarios in the very near future.