Undergoing or undertaking

Developments in the nature and approach of business extortion

Summary

Ilse van Leiden
Tjaza Appelman
Tom van Ham
Henk Ferwerda

Beke reeks

At the request of
Ministerie van Veiligheid en Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Ilse van Leiden, Tjaza Appelman, Tom van Ham en Henk Ferwerda

Undergoing or undertaking

Developments in the nature and approach of business extortion

Summary

Undergoing or undertaking
Developments in the nature and approach of business extortion

Business extortion has many faces. Previous research showed the impact and consequences of extortion on a personal, social and economic level. Based on these findings the Ministry of Security and Justice launched a programmatic approach to business extortion a few years ago. On request of the Research and Documentation Centre (WODC) of the Ministry of Safety and Justice, Bureau Beke evaluated this approach, and the current state of affairs regarding business extortion has been documented.

Research questions and methods

The goal of this research is evaluating whether the launched approach goes according to plan, and whether the measures are still effective to tackle the current extortion problem.

Several research activities were conducted to record this. This includes an international desk research, which contains a media scan, an internet scan, literature research and document research.

In addition, an analysis was made of recorded data from police, the administration of justice and Report Crime Anonymously (Dutch: Meld Misdaad Anoniem). Among nearly 400 businesses an online survey on their knowledge of and their experiences with extortion was conducted; and eight case studies on criminal investigation concerning extortion were carried out. In addition 55 key players of several organizations were interviewed, including police, the Public Prosecutor, organized interest groups, private detective agencies and thirteen victims. To gain an international perspective, experts from eight European countries were inquired about the phenomenon. Furthermore, the research findings were presented to the parties involved in a peer review meeting for consideration.

The phenomenon

In this research business extortion is defined as follows: 'Forcing a (representative of a) company directly or indirectly to issue money, goods or information, whether to contract a debt or to acquit a debt, or to provide certain services or perform actions to benefit oneself or another unlawfully by (threatening with) violence, sabotage, defamation or by revealing information'.

In the Netherlands as well as abroad, extortion of entrepreneurs is still a problem. And the problem has grown in recent years according to several European countries. Perpetrators more and more use modern means of communication to utter threats and make demands. Most extortions are focussed on financial gain. And some victims comply with the demand.

Extortion has massive impact and consequences. Victims are anxious because of the threats and businesses are being harmed. Protection extortion and cyber extortion are current forms of extortion which are increasing internationally. In the case of protection extortion, mainly Outlaw Motorcycle Gangs (OMG's) are involved in the extortion of the hotel and catering industry. By means of intimidation and threats they attempt to infiltrate to make themselves known, to obtain a clubhouse or to create a market for their illegal practices. Protection extortion also exists among ethnic entrepreneurs. However, it is hard to gain insight into this due to the reticence of the Chinese and Turkish community. These types of extortion seem to take place more subtle and on a smaller scale than it did a few years ago. Now, a part of the former cultural extortionists obtain their money probably through criminal activities other than extortion.

Another international development is that the world in which extortion occurs is partly shifting to the online world. Cyber extortion by means of computer hacking, *cryptoware*, *ransomware* or DDoS-attacks is increasing. The rise in cyber extortion can be explained by the increasing availability of such digital means for extortion and the digitization of business. In the case of cyber extortion multiple businesses are often victims simultaneously; and because of the great distance to the perpetrators and their anonymity it is hard to trace them.

A closer look on extortion

Extortion is a hidden delinquency. That means that not all extortion cases are transparent or known.

The actual number of extortion cases involving businesses cannot be determined. Police registrations, verdicts and self-report by businesses give only some indication of the scale of extortion. Yearly, at least 55 extortion cases come to the attention of the police and at least 11 extortion incidents are taken to court. Police statistics as well as judicial statistics show a lower limit since they do not gain

insight into all registered cases. In the survey businesses itself report a bigger scale of the problem and one out of ten businesses indicates to have been a victim of extortion once or multiple times in the past five years. Since the three sources differ in content, quality, representativeness and period of analysis, a comparison of these figures is not possible. These figures can only be considered an indication of the scale of the problem. Indications of the prevalence of extortion in other European countries differ. Self-report by businesses in Finland indicates that two to three percent are victimized and in Sweden between six and eight percent. Because of the different target groups and methods, these figures cannot be compared with the Netherlands. Nevertheless, these findings implicate that extortion is a rather substantial problem to business and that the police has little insight into this matter.

Retailers, service providers and the hotel and catering industry seem to be the most vulnerable branches when it comes to extortion. Since these are the largest branches in the Netherlands, this can account for the relatively large number of victimized businesses in these branches. Also abroad, the retail branch and the hotel and catering industry are characterized as vulnerable branches. Moreover, the construction industry is mentioned as being a target of extortionists due to the building crisis by several European countries. Multiple times, foreign countries also mention collecting debts by means of extortion as the motive behind it.

One-fifth of the entrepreneurs in the survey think of themselves as potential victims. Also one-fifth states to take precautions against extortion, such as camera surveillance or software protection.

Three-quarter of the victim companies who report to the police are Dutch companies. Suspects of reported extortion practices are relatively often former business partners, former clients and former employees. Businesses itself place the blame on criminal groups in particular. However, this offender group hardly comes forward in police registrations. In other European countries, criminal offender groups are also considered important offender groups in the field of extortion. These findings implicate that criminal groups pose a bigger problem for the business community than is known to the police.

The most frequent way to utter threats is confronting the victim face-to-face or through a combination of manners to contact the victim. Businesses are often repeatedly approached by the extortionists. Threatening with violence, defamation, vandalism or revealing information are mostly used to enforce their demands. In most cases an extortionist makes himself known when threatening the victimized company. Money is by far most demanded by extortionists. They demand money for their own financial gain, but also for example to "solve" a (current) business conflict. As a consequence of the extortion businesses suffer mainly on a financial and emotional level.

Detecting, informing and reporting

It is important to notice extortion in time as an extortion process can persist for a long period of time. However, businesses do not always want to come forward on a case like extortion. That is why it is so important that public and private parties know how to recognize extortion. To achieve this, a good state of knowledge on the subject and a warm relationship with businesses based on mutual trust are important. Private parties that could play a role in detecting extortion are the Chamber of Commerce, trade organizations, umbrella organizations and businesses organizations. Within these organisations extortion is normally not a subject of attention so there is no expertise and awareness regarding extortion. However, these parties could play a role because of the natural connection they have with entrepreneurs. Public parties, among which local authorities, the police and the National Cyber Security Centre of the Ministry of Justice can also perform a role in detecting extortion. Signs for extortion can be recognized by these parties in the field or in the digital world. Here are knowledge and awareness essential as well, so coworkers of these organisations know how to recognize signs and which steps to take next. Furthermore professional service providers (for instance, lawyers, accountants and notaries) play a major role regarding detection. More than one-third of the entrepreneurs in the survey state to contact them in case of extortion. Professional service providers have insight into unusual transactions or company takeovers. To improve detection by above mentioned parties, it is important to discuss subjects involving extortion with businesses and to maintain a relationship based on mutual trust.

Detection by other organisations is important since the willingness to inform and report regarding extortion is low. Several factors influence the process of informing and reporting and its progress with the police. First of all businesses do not always see a reason to inform the police in an extortion case, as they do not want go through the process of criminal prosecution. Sometimes companies are satisfied that the extortion ends, or find it sufficient that they can recover the loss through a civil lawsuit. Instead of involving the police, entrepreneurs can also decide to call in a private detective agency. Nevertheless this is often not an option for the smaller businesses, since they do not have the financial means for that.

Other circumstances which play a role in the businesses willingness to inform and report are trust in the police and emotions like shame and fear. Whereas the majority of businesses state to inform the police in case of extortion, a smaller part of businesses does this when they are truly being extorted. Particularly when it comes to cyber extortion, businesses believe that the police are incapable to help them and have too little expertise in this area. Among Turkish and Chinese entrepreneurs, confidence in the police/authorities is low because of their cultural background in particular and the fact that they rather solve their problems within their

own community. Anxiety and feelings of shame result from the fear for retaliation and image harming. Next to the circumstances that influence the victim's willingness to report, there are circumstances within the police organization that influence their willingness to start an investigation. These circumstances are connected with a lack of quality and knowledge regarding extortion and the way victims are treated. For example, the offence that a victim reports is sometimes incorrectly classified and the urgency is not always acknowledged. Other factors that could restrain the informing and reporting process are the critical police's attitude with respect to the victim's story and lack of "professional thinking". Having contacts on an adequate level within the police organization can be conducive to get a good report. Nevertheless, most entrepreneurs have to follow the usual procedure through the public counter. In general, it seems that the police have a passive or reactive attitude towards extortion of businesses. Although there are also examples where the police act proactively by visiting the victim and persuade him to report. The police especially appear to act proactively when criminal groups are involved in the extortion.

Tracing and prosecution

When the police receive a notification or report of extortion they make a decision to take the case or not. Several factors affect this decision. Between notification and investigation of extortion cases exists a phase where the situation has to be evaluated to take the proper next steps. Several experts state that it is important to assist the entrepreneur and advise him after a notification or report.

Important advises are to report and never comply with the extortionists. Sometimes victims get the direct phone number of a neighbourhood policeman or a police officer who they can call if necessary.

In at least four out of ten reported cases a criminal investigation is started. Police's attitude with respect to taking up a case varies from passive to proactive. Many extortion situations fizzle out and in those cases the police will not take action to get an impression of the perpetrator. Usually they also do not invest in tracking down the perpetrator when businesses withdraw or when there is no evidence to investigate. This means that extortion attempts, which are an offence, are often not prosecuted. Cases can also be put off by lack of capacity, low priority or a lack of competence within the organization. Although investigation without a victims report is possible in the case of extortion, this does not happen often.

Within the police organization a case can be taken up on different levels varying from neighbourhood police teams, individual detectives to large-scale criminal investigation teams. The evaluation of the gravity and risks of the situation is conclusive in deciding if a case is upgraded within the police organization. The police have several acting opportunities in an extortion case. Knowledge and expertise appear to be important in order to take proper action. Entrepreneurs have particu-

larly positive experiences with the police when the case is taken up by the criminal investigation department. They pay attention to the victim and are able to make a proper evaluation of the risks. The chance of success of the investigation is improved when the victim gives full cooperation and disclosure. During the investigation the police can decide to a passive strategy in which they take a rather inactive attitude or to an offensive strategy in which action is taken on different levels.

Working towards the physical payment which was demanded is the most extensive strategy where the chance of detaining the extortionists is high. The investigation methods which are used most frequently are investigating a possible suspect, forensic research, observational research, analyzing phone records, tapping telephone lines, studying surveillance camera images and interrogating the victim, witnesses and/or suspect. Social media and digital investigation become an increasingly important part. Recruiting digital detectives and digital expertise is hereby essential. In all cases the safety of the victim has to prevail over tracking down the perpetrators. Furthermore, because of their often distressful situation, victims need direct and honest communication on the developments and outcome of the case. Victims find after-care also important. The extent to which the police pay attention to feedback and after-care however varies strongly.

Within the police organization several services are available to gain expertise regarding extortion cases. These include the central expertise centre for ransom, kidnapping and extortion of the National Police Force, police negotiation teams and specifically for cyber extortion the digital investigators and Team High Tech Crime (THTC). The average police officer has little experience with extortion cases, so it is important that they can make a fast appeal to the proper expertise. In general, the police organization is not very well acquainted with these facilities, so these are not applied in every case.

In a considerable part of the cases investigation results in gaining insight into the suspects, but only in a few cases this results in an arrest. After police intervention victims are often not extorted anymore, but because of lack of evidence a suspect cannot be taken into custody. It appears that those cases are the hardest when a group of offenders is active and when threats are uttered in a face-to-face contact. Every year at least eleven trials involving business extortion take place. Most of these trials result in sentences varying from community service till long-term prison sentences.

Involving the police as soon as possible is one of the factors that contribute to a successful prosecution process. That way the police are able to intervene in the process and to gather evidence during the extortion process.

Approach

In recent years, several projects have been initiated to tackle and prevent extortion. One part of these projects is started by the government and one part by private parties. The National Platform for Crime Control has ordered the committee on extortion to give shape, contents and implementation to a programmatic approach. A part of these projects does not get off the ground, but a number of measurable results have been achieved. The first project is aimed at communicating on extortion towards the target group. The provision of information to the potential victims in the business industry took place on an ad hoc basis and has no structural character. More than two-thirds of the entrepreneurs states not to be informed on extortion. Parties lack the means to communicate about extortion in a structured manner. Encouraging are the developments of the Veilige Horeca app (a tool which was developed to increase the safety in the hotel and catering industry) and the Veilig Ondernemen Scan (a tool which gives businesses insight into the safety risks for their businesses), in which extortion is a separate subject.

The second project was the introduction of an extortion helpline, where entrepreneurs can call an expert anonymously (Dutch: Vertrouwenslijn Afpersing). This extortion helpline started in 2011 as part of improving the relationship with victims on mutual trust. This anonymous helpline appears to (be able to) supply a need. The extortion helpline can be regarded as a potential success in tackling extortion. It is still a potential success, since the project needs continuation and more publicity. Because proper and structural communication about the helpline fails so far, a large and adequate target group is not reached at this moment. Only a small part of the target group is acquainted with the helpline, while the need for such a confidential telephone line for businesses does exist. An important aspect of the telephone helpdesk is that counselors behind the helpdesk meet the victims in person and then guide them to the police or other authorities. Unfortunately, the counselors lack a good network to guide victims quickly towards the adequate persons within the police organization.

Alongside the extortion helpline there is the anonymous helpdesk Report Crime Anonymously of the organization NL Confidential. To stimulate the willingness to report within ethnical communities, NL Confidential contacted this target group on a local level in the third project. The pilot learns that face-to-face contact is effective to get in contact with potential victims and can increase the willingness to report. However, confidence can only be achieved by structural bonding.

The fourth project of the approach is the professionalization of investigating extortion by the police.

A measurable result in the project is the standardization of the national centre of expertise on extortion within the policy plan of the National Police. At the centre of expertise, expert advice can be obtained regarding extortion. The weakness

of the centre of expertise is that it involves only one police officer, so safeguarding knowledge is a point of interest. Furthermore, the centre of expertise is not yet common knowledge within the police organization. This makes that police officers do not appeal to the centre in every case. Other projects regarding the professionalization of the police, such as appointing an Account Manager Intelligence, improving the reporting process or the application of broad expertise have nationwide have not come off the ground. Lack of support for certain points of action is one of the causes.

Nevertheless, in the scope of the fifth project, the field experiment, a number of initiatives regarding the improvement of the reporting process has been developed on a local level. These involve the recording of extortion as a delicate report in the Reporting Handbook of a district, and informing desk clerks on the phenomenon in that same district. In the field experiment, an approach aimed at the target group and district appeared effective to record crime patterns and increase the willingness to report. In order to have a clear picture of the problem, structural monitoring is essential.

In addition to the programmatic approach a few other initiatives were introduced by private parties in particular. This shows that attention to the phenomenon does exist. Several private detective agencies and insurance companies set up report desks and provide information about the different forms of extortion and prevention. Furthermore, there are several insurances available for businesses to insure themselves against the risks and the damage caused by extortion. Extortion also gets attention on an international level. The European Network of law enforcement Advisory Teams (EuNAT) will focus itself for the next two years specifically on the development of expertise in the field of extortion.

Based on the research four themes are designated, which can be considered opportunities for tackling business extortion. These are increasing knowledge and awareness, improving detection and the relationship based on mutual trust, professionalization of the police and a proactive approach. Business and interest groups have a great need for knowledge of extortion. Communicating more often about extortion creates awareness for the phenomenon; businesses will recognize and acknowledge it sooner and they know how to arm themselves against it. This information could be combined in one central online portal. If entrepreneurs or professionals are confronted with extortion, here they can find all required information, such as what extortion signifies, which acting opportunities they have and where to go for help. Therefore the routing must be clear and the police organization has to provide sufficient quality in the reporting process. The latter requires a quality development of the employees at Service and Intake with the police. Other divisions within the police organization require also an increase in knowledge. Especially the possibilities of consulting the centre of expertise on extortion and police negotiators

at extortion cases can be made more public. That way police officers are better able to involve the appropriate expertise in a case.

Another subject which requires an important quality and quantity improvement is cyber extortion.

Digital expertise in the matter of quality and quantity is not optimal at this moment, as is the collaboration between the regional police units and the National Police Force. There is no insight into cases all over the country. In addition, a major point of interest is the internal feedback on cases within the police force and the Public Prosecutor as well as external feedback to victims.

Some forms of extortion require acting more integrally and proactively, as the willingness to report is low although they pose a substantial problem. This applies for instance to extortion by OMG's or cultural extortion, but this can also be an option for new national phenomenon's like cyber extortion. With the launch of an approach aimed at a specific area or nationwide, insight can be gained into the specific forms of extortion. In addition, monitoring the development of extortion could result in faster intervention on certain developments.

www.beke.nl