

Je bedrijf of je leven - Aard en aanpak van afpersing van het bedrijfsleven

Ilse van Leiden, Edo de Vries Robbé en Henk Ferwerda. Advies- en Onderzoeksgroep Beke, 2007

Summary

As a result of (alleged) incidents, business extortion is a subject which has received political attention several times in recent years. In response to this, the Research and Documentation Centre of the Dutch Ministry of Justice (WODC) commissioned Beke Consultancy and Research Group to conduct a (exploring) study of business extortion in the Netherlands. In this chapter the conduct of the research and the major findings from this national study are described in a summary.

Targets, research questions and research methods

The research target is gaining an insight into the way business extortion occurs and develops, to subsequently come to prospects for a successful way to tackle this problem. Three research questions have been formulated on the basis of this target:

1. Which forms of business extortion can we distinguish?
2. What is the nature of (forms of) business extortion?
3. How can we tackle business extortion effectively?

In order to answer these questions we have conducted several research activities including a detailed (international) desk research, nineteen interviews with key figures from various parties, such as the police, the Public Prosecutor, umbrella organisations, trade organisations and employers' organisations, private investigation services and the Regional Platform for Crime Control, as well as three interviews with (representatives of) victim companies.

Furthermore we have discussed and analysed nine criminal investigations of business extortion with crime squads throughout the country.

By making an inventory at the police districts nationwide, a closer insight was gained into the scope and nature of extortion incidents which were recorded by the police.

Finally, the research findings have been tested in two peer supervision meetings with key figures of miscellaneous relevant parties who are able to provide an important input for tackling business extortion. We name for instance the police, Meld Misdaad Anoniem (Report Crime Anonymously), umbrella organisations and trade organisations and private investigation services.

Defining and characterisation

At the outset of the research a working definition of business extortion was formulated, based on relevant sections of the law in which this phenomenon can be included, namely Article 317 (extortion) and Article 318 (blackmail) from the Dutch Criminal Code.

Business community includes large multinationals as well as small-scale businesses and individual employers. An important delimitation is that the research only aims at the bona fide business community. The (working) definition of business extortion is formulated as follows:

Forcing a (representative of a) company directly or indirectly to surrender 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 business extortion, a company, an employer or an employee are threatened to be harmed, if they do not comply with a certain demand. A company can protect itself against the execution of the threats by accepting the extortioner's demand.

This interplay between offender (group) and victim (company) affects the progression of the offence. Extortion can be restricted to a once-only contact between offender and victim, but it can have a more process-oriented character as well. The latter extortion case can be characterised as a 'crime in action', which is a process that lasts longer and is going through various stages. Therefore, this type of offence discerns from many other forms of delinquency such as burglary and murder, which are always accomplished facts.

Targets, motives and consequences

In business extortion, direct or indirect material gain is, in general, a motive of the offender (group). For example, it can involve large amounts of money, acquitting debts or services to enrich oneself.

The offender's motives for committing extortion can be diverse. Financial stringency as well as conflicts or rancour can cause the offender to commit the crime.

To conclude, extortion can be not so much emotionally driven, but it can be a part of the offender's (group) wider criminal repertoire.

Business extortion can be regarded as a serious form of crime, as the consequences can be drastic. The damage caused by extortion or is threatened to be caused, can relate not only to the economic sphere, but to the personal and occasionally even to the social sphere as well. Because of the fact that the management has been disrupted to such an extent by actions of the extortioner, the companies can suffer severe sales loss or image loss, or even go into liquidation.

In addition, a company's representative may be injured in his (feelings of) safety by violence (threats), depending on the form of extortion. In a wider sense this may apply to the victim's family, the company's employees, and even to a large group of customers and consumers. In this last case, public health or social security are being threatened.

Modus Operandi (the way of operating)

Extortioners often select their victim (companies) carefully and contact them through various ways to make their demands. The main methods are sending letters, contacting the victim by telephone, and confronting the victim face-to-face. In many cases a once-only contact is sufficient; in some cases there are multiple contact moments where they use different forms of contacting the victim.

Extortioners enforce their demands with various coercive measures. The coercive measures can be divided into violence, sabotage, revealing information and defamation. (Threatening) violence varies from psychological violence to physical violence by which the victim's feelings of safety are affected. This coercive measure is practically always part of the extortioner's modus operandi (the way of operating).

In sabotage the extortioner threatens to frustrate a company's business conduct and he takes advantage of the companies' fear for sales loss and image loss. Sometimes, sabotage hovers on the borderline of violence.

By threatening with defamation or to reveal delicate information, the extortioner takes advantage of the fear for (personal) image loss as well, depending on the kind of information.

Character

What is the distinctive feature of extortion, and/or which characteristic features can be attributed? Extortion practices can occur consciously anonymous, but offenders can also reveal themselves to the victim company.

Furthermore, extortion incidents can be isolated incidents, but they can have a more structural character as well. When offenders have control of a vital link in a certain industry, extortion has a strategic character.

We can characterise many cases of extortion as parasitical, in which the extortioner unilaterally gains. If both parties would gain of the extortion practices, it is called a symbiotic relationship. Doing business immorally to enrich oneself is such an example. A symbiotic form can eventually lead to a parasitic form.

One last distinction in character concerns the spontaneity by which extortion is committed. It can be an emotionally driven and incidental extortion, or a more conventional form in which the extortion belongs to the offender's (criminal) lifestyle.

Phenomenons

With the typification and the different characters of the phenomenon, business extortion has many faces. Related to the offender's modus operandi, we can name a number of specific phenomenons. These are not exclusive and therefore can show overlap.

One first form is named product extortion. In this form the company's business conduct is sabotaged, for example by (threatening to poison) poisoning perishables, or by placing explosives, if a demand is not satisfied. This form of extortion can be considered a serious violent crime, as public health and national security are being threatened.

A second form of extortion is called protection extortion. In this form a company is being extorted by forcing protection against violence by the offender himself or others, in exchange for payment, goods, services or deeds. This is perchance one of the oldest and most organised professional forms of extortion and it can have a huge impact on the personal and professional atmosphere of the victim (company).

A third form is cyber extortion. In this form the extortioner threatens to make websites on the internet inaccessible, so that companies which are totally dependant on the internet for conducting management, can suffer huge economic loss. Cyber extortion can also occur when companies are pointed out that they have holes in their security network. This creates a new, modern form of protection extortion in which companies are being extorted by forcing protection.

A fourth variant of business extortion is called extortion of individuals. In this form employers are pressured very personally to hand over financial means, goods and services. The consequences for the victim company can be strongly in the personal sphere and have repercussions on management.

The fifth form is extortion of services in which service providers are being extorted professionally to provide services. This form of extortion can be on the verge of doing business immorally (symbiotic extortion).

Vulnerable trades

Extortioners look for weak spots within the business and, based upon this, they will pick a victim. In broad terms, the employers who (traditionally) will not immediately contact the police, are vulnerable to extortion. The same applies to employers who possess much cash and have much to lose. The forms of extortion are related to the type of trade and the type of employer.

First of all, all retailers and the catering industry are vulnerable to the more facing forms of extortion, such as protection extortion and extortion of individuals, because of the open character of these trades.

Furthermore, small companies are also susceptible to extortion as they often do not have the means to take precautionary measures, and as the consequences affect them more personally than it would affect a large concern. The victimship with these types

of companies can also be of a structural nature. Foreign retail and catering employers seem to run higher risk of protection extortion and extortion of individuals.

The larger companies and multinationals are vulnerable to extortion because of the big money circulating and because of the possibility that the company's business conduct can be sabotaged. Product extortion is the biggest risk to the larger concerns. Mostly it involves incidental extortion cases.

Individual business people, service providers and smaller employers are vulnerable to forms like extortion of services and extortion of individuals.

They can be interesting victims for these kinds of extortion, as they can have large amounts of money quickly at their disposal, own other valuable goods like shares, or they can provide interesting services for the criminals. This type of employer is also vulnerable as they can be personally approachable. The risk for structural forms of extortion is also present in this group of employers.

Companies which are totally dependent on the internet, make attractive victims of forms of cyber extortion. Smaller companies whose sales largely depend on online spending are especially vulnerable, as they do not have the security and investigation facilities at their disposal, which larger companies often do have.

Furthermore, every company which does not have adequate security facilities at its disposal, is vulnerable to forms of cyber extortion.

Characterisations of the offender

Based on the research, we can distinct two types of offenders: individual offenders versus group offenders. Individual offenders particularly commit product extortion and forms of extortion of individuals. Depending on the type of offender, extortion of services can also be ascribed to an individual. It can involve former employees or other persons concerned who have confidential company information, but it can involve totally independent operating offenders as well. Many individual extortioners do not operate very professionally. Although they are in fact individual offenders, they can take refuge in the extortion process behind a group or a criminal offender group. Individual extortion usually knows an incidental character, but individuals trying to extort more companies does occur.

In addition to the individual operating extortioner, offender groups are distinguished.

The most prominent offender groups are from the criminal circuit and they mainly commit protection extortion, extortion of individuals and extortion of services.

It is striking that offenders of traditionally foreign origin take an important place in criminal offender groups.

As well as professional offender groups, groups of youngsters can also be considered extortioners. They are mainly engaged in protection extortion in the retail trade and in the catering industry.

Cyber extortionists can operate individually as well as being allied to organized criminal offender groups. The biggest threat appears to come from Eastern Europe, but also in the Netherlands the police have arrested cyber extortionists.

Scale indication

Current statistics on business extortion are rare and give a vague and an incomplete view, which aggravates a reliable scale estimation on the extortion problem. Nevertheless, these statistics indicate the extent of extortion problems. Thus based on current self report statistics from the business community, we can state that the lower limit of the percentage of victimship is 0.14 per cent. In addition, there are sources which indicate a trend of one per cent.

The national screening of registered reports of extortion incidents - as this is conducted in present research in 24 police districts - shows that around eighty extortion incidents come to the notice of the police yearly. This number only concerns an extract of the registrations by which it is an obvious lower limit. Police systems contain more filed extortion cases than we obtained during the inventory.

Based on the self report statistics and the police statistics, it can be stated that business extortion is a serious problem.

Dark Figure

For diverse reasons it can be assumed that there is a substantial dark figure of business extortion. Excepting the fact that an unknown number of extortion cases stays out of the police files, business extortion appears to be, for a major part, a hidden phenomenon for other parties. The features of the victim company, the nature of the offence and the (im)possibilities to inform a party, play an important role in extortion practices staying out of the picture.

It turns out that there is some impediment on a general standard, for going public at all with extortion victimship. This seems to be, for an important part, because of the characteristics of extortion as a crime, in which violence is not eschewed, and because of the consequences of the victim (company) which can be substantial: people are simply fearful to speak about it.

Willingness to report

It was found that there are barriers to report incidents in general, and extortion incidents in particular. The little willingness of employers to report in case of extortion, appears to be connected with several factors. Many factors interact or are found together.

First, there is fear for retaliation of the extortioner, if the victim informs the police.

Secondly, motives pertaining to business economics play a part; one is afraid of image loss and sales loss if the extortion gets out.

Thirdly there is a lack of trust in the police to handle cases carefully and professionally.

One more important aspect is the employers unfamiliarity with extortion as a type of offence, and with the way of acting when they are confronted.

Finally, cultural aspects prove to be connected with willingness to report. Foreign employers in particular, do not inform the police easily. Things like the language barrier, bad experiences, shame and fear for the consequences play a role in this.

Current approach

The current approach of business extortion is restricted to a repressive approach at those moments especially, when the problem occurs evidently, victim companies go public and when they report to the police. From national inventory the police proves to perform investigation efforts in nearly two-third of the cases, when the victim (company) reported.

Investigating extortion incidents is worthwhile as it is found that well over half of these investigation researches result in arresting the suspects.

However, tackling the problem seems to fall short of extortion practices, in which smaller employers are the victim, and of those cases which are never reported.

It can be stated that the attention for business extortion as a problem is found to lack in general.

Future approach

It turns out that the business community is facing extortion practices of which the scale, nature and gravity are in such an order, that a tackling consolidation is valid.

Willingness to this proves to be present in the relevant parties.

To begin with, it is important that business extortion is acknowledged as a problem by all concerned parties, and that it will come up for a theme discussion.

Furthermore it is important to professionalise organisations and processes to create possibilities for an approach. The advancement of expertise regarding extortion as a type of crime and protocolling with regard to procedures are the key concepts.

This professionalising should result in an improved relationship with employers based on trust, a better observation, an increased willingness to report and increased investigation opportunities.

Increasing knowledge (by information) in the business community with regard to extortion and its procedures, is also an essential action item in the approach.

Business extortion invites an integral approach in which it is important to fit in as much as possible, with current structures. It calls for recommendation to try out a similar approach in a pilot (experimental field).