

## The threat of commercial extortion

The threat of extortion is a well-established and ongoing concern facing many commercial organisations throughout the world, where a variety of actors utilise intimidation, threats of violence and disruption in order to extract money, property and other concessions from companies. The threat is particularly prevalent in countries that suffer from large-scale socio-economic disparities, political instability, societal tension or a lack of effective law enforcement. Commercial organisations operating in those environments, particularly foreign-owned companies, are frequently targeted by criminal organisations, disgruntled or disaffected individuals and even terrorist/insurgent groups because of their perceived financial assets. Throughout Latin America, the former Soviet Union, Africa and China, incidents of extortion have grown considerably and show no sign of abating. However, the extortion threat to commercial organisations is by no means confined to troubled countries or developing regions. Even in the developed world, in countries which have established law enforcement and judicial systems, political stability and relative economic prosperity, incidents of commercial extortion occur widely. Adding to the issue is the increase in cyber-based extortion activity in recent years, another indicator that problem shows little sign of abating.

### Extortion defined

Extortion can take many forms, but it is broadly defined as the unlawful extraction of money, property or other concessions through intimidation, threats or menaces. The menace can involve diverse and sometimes inventive threats to either damage assets or reputations, or cause harm or distress to individuals. The threats may involve, but are by no means limited to, the use of explosive devices, arson, computer viruses/malware/hacking, communication sabotage, assault, kidnapping, malicious product contamination or industrial espionage. The threat can also be to reveal propriety data or customer data, or to expose alleged indiscretions by employees or immoral/unethical

behaviour and business practices. The demands in an extortion attempt may simply be monetary, but can also be activity orientated; extortionists may demand that a company ceases operations or controversial practices/decisions, such as making large-scale redundancies. The motive may also vary from criminal financial reward to putting a competitor out of business, further a political or criminal objective, gain publicity or secure a financial reward.

The profile of extortionists is also highly varied. Perpetrators may range from terrorist/insurgent groups, drug cartels and other large criminal organisations, to politically-motivated activists and disaffected employees/individuals who may hold a grudge against an organisation. An extortionist's state of mind may vary from cold, calculated and highly organised to the unpredictable and extremely deranged. Terrorist/insurgent groups and large, well-established criminal gangs can exert considerable menace by their reputations alone. As with financially-motivated individuals, these groups will also often go to considerable lengths to convince their victim of their capability to carry out their threats. These groups frequently have an extensive reach and are capable of organising acts of extreme violence or significant disruption. Criminal gangs and other financially-motivated groups and individuals are likely to act



One of the more common motives of extortion is financial gain.

discreetly, at least initially. However, not all offenders will act with such inconspicuous subtlety. Politically-motivated extortionists, such as animal rights or environmental activists for example, will often actively seek publicity. As with other offenders, such groups are likely to be highly-motivated and intimidating and their demands may frequently be outside the scope of what their victims can deliver.

Extortionists that are psychologically ill or who harbour a deep-seated grudge can also be particularly difficult. The motives behind their threats may be unclear and negotiations can be complex, with irrational or unachievable demands. The unpredictable nature of the perpetrator also means that threats may be carried out without warning or thought for the consequences.

### Established threats and emerging trends

Although reliable extortion statistics are difficult to obtain for several reasons (many extortions are not reported out of distrust of the authorities; fear of the consequences; and a desire to avoid publicity and potential damage to their brand and reputation), it is estimated that the annual number of extortion incidents is increasing on a worldwide basis. Unstable and developing regions continue to pose the greatest risk to companies, but even organisations operating in what are seen as 'First World' countries can regularly be threatened by extortionists. For example, according to the risk management, reinsurance and human capital consulting firm, Aon, there were an average of 23 commercial extortion cases reported each year in the UK between 2003 and 2006. In 2007, this figure rose to 40 incidents and in the period August 2007 to August 2008, there were some 67 reported cases. The problem is particularly prevalent in Northern Ireland. According to the Police Service of Northern Ireland (PSNI), the level of paramilitary rackets has increased markedly since the Good Friday Peace Agreement of 1998. Some businesses are now forced to pay up to £10,000 (USD\$20,000) a month to paramilitary organisations who use their terrorist credentials to threaten and intimidate companies for 'protection money'. A similar extortion problem can be found in the Basque country in France and Spain. Euskadi

Ta Askatasuna (ETA) has long used extortion, in the guise of 'revolutionary taxes', to fund its 40-year-old separatist campaign. Companies that refuse to pay have often had their businesses blown up or their employees and their families threatened. Commercial extortion is also prevalent in Italy, with various Mafioso groups securing millions of dollars each year through protection money and bribery, and in Japan, where corporate extortion, known as sokaiya, typically takes the form of threats to a company's shareholder unless a payment is made.



The profile of extortionists is highly varied and can range from criminal and terrorist groups to disaffected individuals.

Although traditional physical threats continue to make up the vast majority of extortion incidents, technology and the internet is now leading to new avenues of extortion. Computers and the worldwide web enable individuals or small groups, frequently located hundreds, if not thousands, of kilometres away to extort money from an organisation without threatening violence or stepping foot on the premises. However, cyber-based extortion can still result in significant damage and disruption to a company's operation and reputation. As with traditional extortion schemes, cyber-extortion attacks can vary hugely in terms of sophistication. At one end of the spectrum, criminals use the relatively simple and crude mechanism of manufacturing a fake site on the internet purporting to be that of a legitimate company, but containing pornographic material. A payment is then demanded for the site to be closed. A more advanced scheme is for criminals to launch a denial of service attack

on a website, frequently against companies who use the web as a high-volume trading platform (such as online gambling sites), thereafter requesting a payment to stop the technological assault. At the very highest end, hackers can gain access to a company's propriety information, financial data and personnel files which can then be used to leverage significant financial concessions under the threat of revealing the information to competitors or the media. Such is the success of such extortion activities that there is now evidence of organised criminal groups and terrorist/insurgent organisations recruiting or sponsoring hackers and virus creators to work for them. For example, Russian mafia groups have recruited computer experts from the Ukraine, Romania and Bulgaria to launch cyber-extortion attacks against targets both within the former Soviet Union and abroad.

### Advice and Assistance

Whether a company faces a traditional extortion attempt in an unstable and high-risk security environment or a cyber-extortion attack in the developed world, such incidents can have a significant impact on a company's operation or profits. As a consequence, all organisations would be well advised to develop and implement robust crisis management plans and processes that are capable of dealing with such eventualities. Companies should start by making a comprehensive and realistic baseline assessment of the threats and vulnerabilities both within and outside the organisation. A security survey or audit should evaluate the security environment in which a company operates identifying key threats and trends. Shifts in political, social and economic dynamics or changes to the ethnic and cultural landscape, for example, can also bring about dramatic changes to previously benign security environments. Companies must also assess their internal processes and evaluate their key corporate interests and assets. In doing this, companies will identify areas of weakness and concern and they can then act appropriately.

Commercial organisations should also formally establish a Crisis Management Team (CMT). This team must consist of senior personnel with the correct and complimentary skill sets to deal effectively with a crisis, such as an extortion attempt. Members of any CMT must also understand their own roles and duties before, during and after a crisis incident, as well as the roles and duties of other CMT members. Individuals on the team need to understand and appreciate the pressures that they will face and how to deal with them. All plans, procedures and processes need to be robustly tested. Companies should undertake simulated incident training that will introduce their key personnel to the mechanics of an extortion attempt/crisis preferably in consultation with a specialist firm that can advise and direct such activities. A live extortion or crisis incident makes a very poor learning environment and without experience, mistakes are inevitable and can result in serious damage to a company's brand, reputation and profitability. Realistic, scenario-based, exercises enhance an organisation's ability to respond to a crisis incident and will enable CMTs to act in a professional, carefully orchestrated, coordinated and effective manner.

---

Clinton Brannigan, Global Security Specialist at red24, looks at the issue of commercial extortion. red24 offers a holistic, multi-faceted extortion prevention and response service that can minimise the threats to organisations and reduce or eliminate damage and disruption in the event of an actual extortion attempt. Our team of security specialists have significant experience in extortion prevention, negotiation, investigation and resolution and can provide comprehensive risk and threat assessments, crisis management planning and training. For more information on the services and assistance red24 can provide in this regard, please contact [customerenquiry@red24.info](mailto:customerenquiry@red24.info)

---