Technology and the evolution of extortive crime

By Joseph Smith
Compiled with data from CORE

As technology continues to change the nature of modern life and business, so crises continue to evolve in both sophistication and complexity. Kidnapping has long been one of the highest-impact crimes for companies and their personnel, but a host of additional perils now have the potential to disrupt business. Technological advances are not only enabling new dangers to flourish, but also changing the ways in which old ones manifest. As criminal activities evolve at an ever quickening pace, corporate responses must keep up.

Evolving threats

Extortive crime has always been a hazard of doing business in many parts of the world. It has ranged from petty attempts to demand money with menaces to more serious manifestations, such as the potentially lethal contamination of a company's products or the kidnapping of its staff.

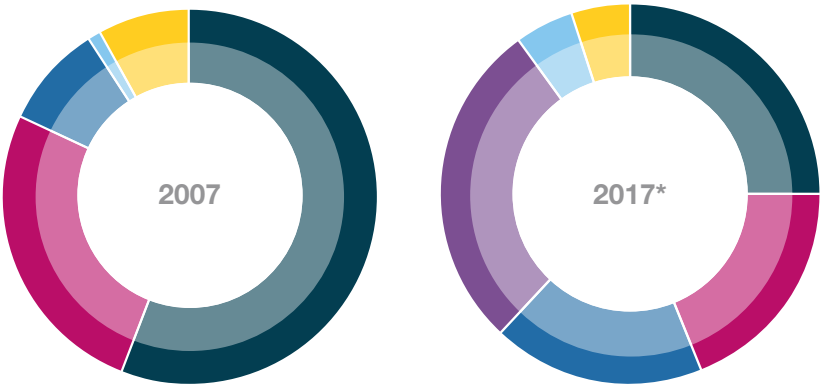
A decade ago, more than half of the threat to life or extortive crises our clients encountered involved the kidnap-for-ransom of an employee or relative. In the intervening years, the total number of kidnaps has never once fallen below 2007 levels. Alongside the growth of kidnapping-for-ransom, Control Risks has seen a 397% increase in threats, extortions, cyber extortions and other international problems since 2007. Given that these represent just those cases reported to Control Risks, it is reasonable to assume that the real rise in incidents is much greater.

Source: Control Risks CORE © Control Risks 2017

Fig.1 ▶ Threat to life or extortive case breakdown 2007 vs 2017

Threat to life	2007	2017	Key
Kidnap	56%	25%	
Threat Extortion	26%	19%	
Threat	9%	18%	
Cyber	0%	28%	
Detention	1%	5%	
Other	8%	5%	

***2017 data covers January to November, while 2007 data covers January to December**



Technological innovation

The single biggest reason for the increase in other hazards is technological innovation. Like businesses, criminals have long had the ability to diversify and adapt to changes in their operating environments. They continually learn new techniques and acquire new tools to minimise the risks they face while maximising their potential rewards. Innovation and evolution have accelerated as digitalisation and increased connectivity have created myriad tools and opportunities for tech-savvy criminals. They have also revealed new vulnerabilities for businesses.

In addition to their personnel and physical assets, organisations hold vast amounts of data, including intellectual property with a high monetary value and sensitive client details with the potential to cause significant reputational damage. As corporations seek to protect themselves from these new vulnerabilities, criminals have at their disposal an array of new methods to exploit them. These range from small-scale phishing activities, to headline-grabbing ransomware attacks and global data breaches.

In the information age, new criminal opportunities are not open to cyber specialists alone. Intimate details of employees and businesses are readily available online for malicious actors to use against them. Rather than carrying out a period of surveillance to identify a target's address, routines and proclivities, an extortionist may simply need access to their social media profile, their employer's website or even just their telephone number.

New protagonists

As well as creating new opportunities for seasoned criminals, the technological revolution has opened up extortive crime to a new type of protagonist. The decision to kidnap somebody or cause life-changing harm requires criminal intent and the ability to set aside significant moral scruples. By contrast, extortion, threats or digital crime are open to a multitude of people who would never dream of wielding a weapon, but have no compunction about causing financial and reputational loss, or psychological stress and trauma.

While many extortionists still have the capability to carry out their threats, many do not. Their target is left to assess whether the threat is empty, or whether the perpetrator genuinely has the intent and capability to carry it out. Unlike kidnapping, extortion is not bound by what is possible, but instead by what is credible. Rather than actually causing physical harm, extortionists simply have to claim convincingly that they can and will do so, or already have.

Virtual kidnapping has evolved in this way. Rather than abducting someone and demanding a ransom for their release, extortionists have learned that they can simply convince the alleged victim's family or employer that a kidnap has occurred to elicit a ransom payment. An extortionist hopes that their target will be scared enough to pay up before they are able to make contact with the alleged victim and realise that no kidnap has taken place. Often, the perpetrators operate from behind bars and at a great distance from their targets. Geographical confines are no obstacle to this brand of extortion; the same is true for many others.

Crisis response

The challenge for organisations confronted by these issues is managing the uncertainty, ascertaining whether the threat is real and knowing how to respond. This is difficult because the threats that are delivered – with or without extortive demands – remain credible the world over. After all, highly capable and feared criminal or terrorist groups, as well as lone malicious actors, can follow through on threats in many circumstances.

A response to this broadening array of crimes must reflect the swiftly changing motives, capabilities and profiles of their perpetrators. This means keeping one step ahead of the rapid advances in technology that criminals use to ply their trade. It also means applying a wider range of tools, and providing a holistic, multidisciplinary response to help organisations to feel comfortable with, or indeed reduce, the ambiguity that modern crises can present.

Take, for example, an aggrieved customer who makes a series of calls to a company threatening to blow up one of its facilities unless demands for a refund are met. Unlike with a kidnap, the protagonist's capability and intent are not proven at the outset. However, a comprehensive background investigation that discovers that the customer has a criminal record, a history of anger management or impulse control issues, and access to firearms would alter an assessment of the threat. In an alternative scenario, the extortionist might attempt to conceal their identity by using an encrypted email provider to issue their violent threats. Dark web searches may reveal that the email account was linked to a cybercriminal network involved in low-level money-making schemes. This could seriously undermine the extortionist's professed ability to carry out their threats, allowing the business to return to normal.

Managing the crises of the future

From the amateurish to the sophisticated, traditional forms of extortive and high-impact crime will always be a problem. Digitalisation and connectivity mean those who seek to gain through extortive and high-impact crime now have greater opportunity and ability to do harm. The threat landscape will continue to develop and become more complex with rapid technological change, but traditional principles of crisis management will always form the foundations of any response. Keeping abreast of the rapidly evolving perils that threaten modern business will be integral to successfully overcoming the crises of the future.

Joseph Smith

Analyst

joseph.smith@controlrisks.com

About Control Risks CORE

CORE provides incisive analysis and forecasting on geopolitical and security issues, comprehensive country risk ratings, an extensive database of incidents, plus visualisation and analytics tools.