Organized Crime and Cyber-Crime: Implications for Business

Phil Williams, CERT® Coordination Center

Introduction

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted while also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography and pedophile rings, but also drug trafficking and criminal organizations that are more concerned about exploitation than the kind of disruption that is the focus of the intruder community. In the virtual world, as in the real world, most criminal activities are initiated by individuals or small groups and can best be understood as "disorganized crime." Yet there is growing evidence that organized crime groups or mafias are exploiting the new opportunities offered by the Internet. Organized crime and cyber-crime will never be synonymous – most organized crime will continue to operate in the real world rather than the cyber-world and most cyber-crime will continue to be the result of individuals rather than criminal organizations per se. Nevertheless, the degree of overlap between the two phenomena is likely to increase considerably in the next few years. This is something that needs to be recognized by business and government as an emerging and very serious threat to cyber-security. Accordingly, this analysis sets out to do three things:

1. Explain why the Internet is so attractive to criminals in general and to criminal organizations in particular.

2. Identify some clearly discernible trends that provide important clues about ways in which organized crime and cyber-crime are beginning to overlap.

3. Identify a series of measures necessary for business to respond effectively to the growing exploitation of the Internet by organized criminals.

Organized Crime and Cyber-Crime

Organized crime is primarily about the pursuit of profit and can be understood in Clausewitzian[1] terms as a continuation of business by criminal means. Criminal organizations are not the only players in illicit markets, but they are often the most important, not least because of the added "competitiveness" that is provided by the threat of organized violence. Moreover, criminal organizations tend to be exceptionally good at environmental scanning in the search for new criminal enterprises and activities. In this context, the Internet and the continuing growth of electronic commerce offer enormous new opportunities.

[1] [Editor's note: Carl Phillip Gottleib von Clausewitz (1780-1831) was a Prussian soldier and intellectual who wrote a book on military strategy entitled *On War*.]

In recent years, there has been a massive increase in the sophistication of organized crime and drug trafficking groups. Colombian drug trafficking organizations, for example, have followed standard business practices for market and product diversification. Criminal organizations have increasingly hired financial specialists to conduct their money laundering transactions. This adds an extra layer of insulation while utilizing legal and financial experts knowledgeable about the layering of financial transactions and the availability of safe havens in offshore financial jurisdictions. Similarly, organized crime does not need to develop technical expertise about the Internet; it can hire those in the intruder community who do have the expertise, ensuring through a mixture of rewards and threats that they carry out their assigned tasks effectively and efficiently.

Organized crime groups typically have a home base in nations that provide safe havens from which they conduct their transnational operations, such as various kinds of trafficking activities. In effect, this provides an added degree of protection against law enforcement and allows them to operate with minimal risk. The inherently transnational nature of the Internet fits perfectly into this model of activity and the effort to maximize profits within an acceptable degree of risk. In the virtual world there are no borders (a characteristics that makes it very attractive for criminal activity); yet when it comes to policing this virtual world borders and national jurisdictions loom large – making large-scale investigation slow and tedious at best, and impossible at worst.

The Internet itself provides opportunities for various kinds of theft. Online thieves can rob online banks or illicitly gain access to intellectual property. The Internet offers new means of committing old crimes such as fraud, and offers new vulnerabilities relating to communications and data that provide attractive targets for extortion, a crime that has always been a staple of organized crime.

The anonymity of the Internet also makes it an ideal channel and instrument for many organized crime activities. The notion of a criminal underworld connotes a murkiness or lack of transparency, where who is doing what is usually hidden from view. Secrecy is a key part of organized crime strategy and the Internet offers excellent opportunities for its maintenance. Actions can be hidden behind a veil of anonymity that can range from the use of ubiquitous cyber-cafes to sophisticated efforts to cover Internet routing.

Organized crime has always selected particular industries as targets for infiltration and the exercise of illicit influence. In the past, these have included the New York garbage hauling and construction industries and the Fulton Fish Market, the toxic waste disposal and construction industries in Italy, and the banking sector and aluminum industry in Russia. From an organized crime perspective, the Internet and the growth of e-commerce can be understood as the provision of a new set of targets for infiltration and the exercise of influence – a prospect that suggests that

Internet technology and service firms should be particularly careful about prospective partners and financial supporters.

In sum, the synergy between organized crime and the Internet is not only very natural but also one that is likely to flourish and develop even further in the future. The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more. It is critical, therefore, to identify some of the ways in which organized crime is already overlapping with cyber-crime.

Major Trends in Organized Crime and Cyber-Crime

The first trend is that organized crime groups use the Internet for major fraud and theft activities. Perhaps the most notable example of this – albeit an unsuccessful one – occurred in October 2000 and concerned the Bank of Sicily. A group of about 20 people, some of whom were connected to mafia families, working with an insider, created a digital clone of the Bank's online component. It then planned to use this to divert about $400 million allocated by the European Union to regional projects in Sicily. The money was to be laundered through various financial institutions, including the Vatican bank and banks in Switzerland and Portugal. The scheme was foiled when one member of the group informed the authorities. Nevertheless, it revealed very clearly that organized crime sees enormous opportunities for profit stemming from the growth of electronic banking and electronic commerce.

Indeed, organized crime diversification into various forms of cyber-crime or Internet related crime is closely related to a second discernible trend – organized crime involvement in what was once categorized as white collar crime. The activities of the US mob and Russian criminal organizations on Wall Street fall into this category: during the late 1990s there were numerous cases of criminal organizations manipulating micro-cap stocks using classic "pump and dump" techniques. While much of this was done through coercion or control of brokerage houses, the Internet was also used to diffuse information that artificially inflated the price of the stocks. Among those involved were members of the Bonnano, Genovese, and Colombo crime families as well as Russian immigrant members of the Bor organized crime group. As criminal organizations move away from their more traditional "strong arm" activities and increasingly focus on opportunities for white collar or financial crime, then Internet-based activities will become even more prevalent. Since Internet-related stock fraud results in $10 billion per year loss to investors, it offers a particularly lucrative area for organized crime involvement.

This is not to suggest that organized crime will change its character. Its inherent willingness to use force and intimidation is well suited to the development of sophisticated cyber-extortion schemes that threaten to disrupt information and communication systems and destroy data. Indeed, the growth of cyber-extortion is a third significant trend. Although extortion schemes — as the Bloomberg[2] case showed — are sometimes bungled, they can be done in ways that incur only modest risks (because of anonymity) and yield high pay-offs. Indeed, this might already be a form of crime that is significantly under-reported. Yet it is also one that we can expect to see expand considerably as organized crime moves enthusiastically to exploit the new vulnerabilities that come with increased reliance on networked systems.

A fourth trend is the use of what were initially nuisance tools for more overtly criminal activities. Perhaps the most notable example of this occurred in Fall 2000 when a variation of the Love Letter worm was used in an effort to gain access to account passwords in the Union Bank of Switzerland and at least two banks in the United States. Although this episode received little attention – and it is not entirely clear who the perpetrators were, it gives added credence to the point made above that there is a growing relationship between organized crime and intruders who provide the technical expertise.

A fifth trend that we can expect to see is what might be termed jurisdictional arbitrage. Cyber-crimes – certainly when they are linked to organized crime – will increasingly be initiated from jurisdictions that have few if any laws directed against cyber-crime and/or little capacity to enforce laws against cyber-crime. This was one of the lessons of the Love Bug virus. Although the virus spread worldwide and cost business billions of dollars, when FBI agents succeeded in identifying the perpetrator, a student in the Philippines, they also found that there were no laws under which he could be prosecuted. Although more and more countries (including the Philippines) are passing legislation dealing with cyber-crime, there will continue to be what have been termed jurisdictional voids from which criminals and intruders can operate with impunity. Indeed, it is possible that some jurisdictions will increasingly seek to exploit a permissive attitude to attract business, creating both information safe havens (paralleling offshore tax havens and bank secrecy jurisdictions) that make it difficult for law enforcement to follow information trails and insulated cyber-business operations.

A sixth trend is that the Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place the opportunities for laundering money through over-invoicing and under-invoicing are likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases, laundering money by paying much more than the goods are worth. Online gambling also makes it possible to move money – especially to offshore financial centers in the Caribbean. Moreover, as e-money and electronic banking become more widespread, the opportunities to conceal the movement of the proceeds of crime in an increasing pool of illegal transactions are also likely to grow.

[2] [Editor's note: Michael Bloomberg, founder of Bloomberg L.P, an information services, news, and media company, worked with the FBI in a sting operation to apprehend cyber-extortionists, who were arrested in August 2000.]

A seventh trend is what might be termed growing network connections between hackers or small-time criminals and organized crime. In September 1999, for example, two members of a group known as the "Phonemasters" were jailed for two years and 41 months respectively. They had penetrated the computer systems of MCI, Sprint, AT&T, and Equifax. One of them, Calvin Cantrell had downloaded thousands of Sprint calling card numbers that were sold to a Canadian who passed them to someone in Ohio, from whom they went to an individual in Switzerland and subsequently to organized crime groups in Italy. As well as intruders working directly for criminals, these network connections between the two kinds of groups are likely both to deepen and to widen.

In addition, of course, organized crime groups use the Internet for communications (usually encrypted) and for any other purposes when they see it as useful and profitable. Indeed, organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as it is many other opportunities for illegal activity. The implications are far-reaching and require a response not only from governments but also from businesses that can all too easily become the targets of organized crime and cyber-crime.

Implications for Business

The implications of all this for business are far-reaching. They suggest that there is a need for major changes in thinking about cyber-security and in planning and implementing security measures. These are particularly important if e-commerce is to reach its full potential and if individual companies are to avoid significant losses as a result of criminal activities. Perhaps the most important changes are in thinking. This has two distinct but overlapping dimensions: security has to be understood in broad rather than narrow terms, and security can no longer be an after-thought, but needs to be part of intelligence, planning, and business strategy. With this in mind, there are several specific recommendations that need to be considered carefully by firms in the high-tech sector.

1. Recognize the real problem is crime, not hacking

Organized crime and cyber-crime are becoming an increasingly salient component of the business environment. Disruption, denial of service, and web site defacements will continue to be problems, but exploitation of access to information systems for profit is likely to become more pervasive. The trend towards accessing business systems, highlighting security holes, and offering one's services for a significant fee, for example, is a thinly veiled form of extortion. As such, it is very difficult from traditional hacking that is designed to highlight security problems and ways of dealing with them as simply a demonstration of expertise.

2. Business intelligence needs to include criminal intelligence analysis

Indeed, criminal intelligence analysis needs to be integrated fully into business intelligence; risk assessment needs to incorporate criminal threats; and cyber-security needs to be conceptualized as part of a broader security problem that cannot be understood or dealt with in strictly technical terms. Defending against such contingencies requires that high-tech firms develop broad security programs that incorporate cyber-security into a much broader program. Cyber-security needs to be one component of a broader security program that includes personnel, physical assets, the provision of services, and financial assets. An arrangement in which the security officer is responsible for cyber-security as part of a comprehensive mandate is likely to be more effective and appropriate than one in which cyber-security is seen as a distinct portfolio separate from other components of security.

3. Beware of infiltration

If cyber-extortion is likely to be a growing problem, another danger is that the high-tech industry is vulnerable to infiltration by organized crime, especially when seeking foreign partners. Consequently, the kind of due diligence exercise that has long been common in the banking sector needs to be extended to other industries. For bankers "know your customer" has become standard practice. For the hi-tech business, it is perhaps even more important to know your partners, especially when they are from another country. Questions need to be asked about their financing, their clients, and their associates – as well as the extent to which there are laws against cyber-crimes. Thorough background checks are essential prior to allowing any joint use of data and communication systems, or to bringing in their representatives to work with one's own employees. When there is overseas expansion, these background checks need to be extended to new employees and consultants. Although this might appear to be an exaggerated concern, it is not. One characteristic of Russian organized crime, in particular, is the systematic way in which it has infiltrated and, in some cases, come to dominate particular economic sectors, often operating through apparently legitimate front companies. Organized crime has infiltrated large parts of the Russian banking system, dominates the energy sectors in St. Petersburg, and has made great inroads into the hotel system. There is no reason that the high-tech sector should be exempt. Indeed, Mikhail Cherny, a well-known Russian entrepreneur with a very dubious reputation, was expelled from Bulgaria in the summer of 2000. He had a controlling interest in Mobiltel, the largest provider of cellular telephones in the country, and had been engaged in several fraudulent activities as well as suspected money laundering. Although the dangers are greater when companies operate in other countries, even in the United States there are problems with organized crime. Russian criminals in the United States, for example, operate through émigré networks, and there is a growing Russian presence in the information technology sector that could very easily be connected in some ways to Russian organized crime.

4. Be sensitive to money laundering opportunities

Companies offering financial services on the Internet – and particularly those offering mechanisms to facilitate financial transactions – need to take steps to identify opportunities for money laundering. Once this is done, they need to introduce safeguards to close loopholes and prevent money laundering. The more this is done by the firms themselves, the less likely they are to be embarrassed and the less likely they will be subject to government regulation.

5. Develop partnerships and information-sharing arrangements

Another response to the growing overlap between organized crime and cyber-crime is to develop a working partnership with government and law enforcement agencies. Once again, there are precedents for this in other sectors. In recent years, the major oil companies, although very competitive with one another, established information sharing arrangements and worked very closely with law enforcement to minimize infiltration by organized crime figures and criminal companies. Government-private sector cooperation of this kind is not always easy, and has been particularly fraught in the area of information security, particularly regarding the issue of reporting. There is broad agreement that cyber-crime is under-reported. One of the most important – and understandable – reasons is concern on the part of financial institutions and businesses about reputational damage. For e-commerce to continue to expand rapidly, transactions must be perceived to be secure – and there is a natural desire to avoid any disclosures that might undermine customer confidence and place a company at a competitive disadvantage. Unfortunately, this reticence works in favor of the criminals. There are three levels at which the disclosure issue can be understood: within the business sector itself, the relationship between business and law enforcement, and full public disclosure. Indeed, the more the first two options are developed and refined, the less need there will be for full public disclosure. One useful approach, therefore, would be for companies within a particular sector to agree to share information about cyber-crimes among themselves, on the assumption that similar methods and techniques that are used against one are also likely to be used against others. Even more important though is the development of mutual trust between business and law enforcement. Indeed, there are several instances of companies working closely with law enforcement in responding to cyber-threats. Perhaps the classic example is the failed effort to extort Bloomberg. The head of the company worked closely with the FBI and participated in a sting operation that led to the arrest of the extortionists. For cooperation to be effective, however, law enforcement agencies have to exercise considerable care and discretion not to expose company vulnerabilities, while the companies themselves have to be willing to report any criminal activities directed against their information and communication systems.

None of these measures is a panacea. Nevertheless, each one can be understood as a key element of what needs to be a comprehensive response. Individual firms obviously have to tailor their security programs to their particular vulnerabilities and needs. Unless they recognize that organized crime and cyber-crime are becoming more convergent, however, their programs are unlikely to be sufficient.